On Hamilton cycle decompositions of r-uniform r-partite hypergraphs

Michael W. Schroeder

Marshall University, Huntington, WV, USA
Email Address: schroederm@marshall.edu

Abstract

The definition of edge-adjacency can be generalized in multiple ways to hypergraphs, and extended from that, cycles and Hamilton cycles. One such generalization of a Hamilton cycle is attributed to Kierstead and Katona. In a recent paper by Kuhl and Schroeder, Hamilton cycle decompositions of complete r-partite r-uniform hypergraphs are discussed, a conjecture was made that the necessary numerical conditions are sufficient, and was shown true for some cases. In this paper, the conjecture is proved using constructions involving Hamming codes, comparisons between the two constructions are made, and a classification of when they are equivalent is shown.

1 Introduction

Let $G = G(V, E)$ be a graph whose vertex set V has n vertices and an edge set E. A *decomposition* of G is a partitioning of E. A *Hamilton cycle decomposition* of G is a decomposition of G into Hamilton cycles. The existence of Hamilton cycle decompositions for K_n (n odd) and $K_n - F$ (n even and F a 1-factor) was classified in the late 19th century by Walecki [6]. Such decompositions are also known for bipartite graphs $K_{n,n}$ (n even) and $K_{n,n} - F$ (n odd and F a bipartite 1-factor) [3].

Let G be an r-uniform hypergraph with $V = \{v_0, \ldots, v_{n-1}\}$. Berge [2] generalized the definition of a Hamilton cycle H as a sequence of vertices and hyperedges

$$H = (v_0, e_1, v_1, e_2, v_2 \ldots, v_{n-1}, e_n, v_0),$$

where v_i and v_{i-1} are incident with e_i ($1 \leq i \leq n-1$), v_{n-1} and v_0 are incident with e_n, and $e_1, e_2 \ldots, e_n$ are distinct hyperedges. A classification of complete 3-uniform hypergraphs (also minus a 1-factor) was completed in 1994 by Verrall [9].

Kierstead and Katona [4] introduced an alternative generalization of a Hamilton cycle; a Hamilton cycle H is represented by a sequence of vertices of G

$$H = (v_0, v_1, \ldots, v_{n-1}, v_0)$$

where the hyperedge $\{v_i, v_{i+1}, \ldots, v_{i+r-1}\}$ (indices taken modulo n) is an edge of H for each $i \in \mathbb{Z}_n$. Meszka and Rosa [7], along with Bailey and Stevens [1], investigated the existence of a Hamilton cycle decomposition of the complete r-uniform hypergraph $K_n^{(r)}$ for various n and r using this of a Hamilton cycle. We will use this definition for the duration of the paper.

Let $K_{r\times m}^{(r)}$ denote the complete balanced r-uniform r-partite graph, whose vertex set consists of r parts, each having m vertices, and whose edge set consists of all subsets of vertices containing exactly one vertex from each part. Thus $K_{r\times m}^{(r)}$ has rm vertices and m^r edges, so a necessary condition for the existence of a Hamilton cycle decomposition is r dividing m^{r-1}. In [5], this condition is shown to be sufficient for all applicable m when r is prime, r is a product of distinct primes, or $r = 4$. Additionally, it is shown that such a decomposition exists if r divides m, and it is conjectured that the necessary divisibility condition is sufficient. In this paper, we briefly rehash some of the methods from [5] and prove the conjecture.

In Section 2, we discuss a relationship between decompositions of $K_{r\times m}^{(r)}$ and partitions of $\mathbb{Z}_m^{r-1}$. We strengthen the conjecture involving these partitions and reduce it to cases when m is the largest square-free integer dividing r. In Section 3, we prove the conjecture when r is a power of a prime, then prove the conjecture when r is any composite integer. In Section 4, we review the constructions used in [5] and show they are equivalent to the ones used in this paper for certain cases.

2 Definitions and Background

Let $r \geq 2$ and $m \geq 2$ be given and let $G = K_{r\times m}^{(r)}$. Let $V^0, V^1, \ldots, V^{r-1}$ denote the partite sets of $V(G)$, with $V^i = \{0^i, 1^i, \ldots, (m-1)^i\}$. To each vertex of V^i, we associate its *value* to the corresponding element of the quotient ring $\mathbb{Z}_m$; the use of the superscript indicates a vertex and its absence indicates its value. For each $i \in \mathbb{Z}_r$, we use $a_{i,0}, a_{i,1}, \ldots, a_{i,m-1}$ to be an ordering of the elements of $\mathbb{Z}_m$, and hence $a_{i,0}^i, a_{i,1}^i, \ldots, a_{i,m-1}^i$ is an ordering of the vertices in V^i.

The edges of G are all r-subsets of V containing a unique vertex from each V^i, and hence $|E(G)| = m^r$. An r-tuple of $\mathbb{Z}_m^r$ may be associated to each edge of G:

$$\{v_0^0, v_1^1, \ldots, v_{r-1}^{r-1}\} \in E(G) \longleftrightarrow (v_0, v_1, \ldots, v_{r-1}) \in \mathbb{Z}_m^r.$$

A Hamilton cycle H of G is necessarily of the form

$$\begin{aligned} H \;=\; (& a^0_{0,0}, a^1_{1,0}, \ldots, a^{r-1}_{r-1,0}, \\ & a^0_{0,1}, a^1_{1,1}, \ldots, a^{r-1}_{r-1,1}, \\ & \vdots \\ & a^0_{0,m-1}, a^1_{1,m-1}, \ldots, a^{r-1}_{r-1,m-1}, a^0_{0,0}\ ). \end{aligned} \tag{1}$$

Throughout this paper, we use e_i to mean a vector with 1 in the ith entry and zero everywhere else. Additionally, we use $[n]$ to denote the positive integers $\{1, \ldots, n\}$. Now, we give a series of definitions along with restating a version of a useful lemma from [5].

Definition 2.1. Let $e = (x_0, \ldots, x_{r-1}) \in \mathbb{Z}_m^r$ represent an edge of G. Then the *difference type* of e is an $(r-1)$-tuple given by $(x_1 - x_0, \ldots, x_{r-1} - x_{r-2}) \in \mathbb{Z}_m^{r-1}$.

Definition 2.2. The Hamilton cycle H in (1) is *cyclic* if there exists a *difference* $d \in \mathbb{Z}_m$ such that $a_{i,j} - a_{i,j+1} = d$ for each $i \in \mathbb{Z}_r$ and $j \in \mathbb{Z}_m$. This is equivalent to $a_{i,j} = a_{i,0} - jd$ for each $i \in \mathbb{Z}_r$ and $j \in \mathbb{Z}_m$. Thus d is a unit of $\mathbb{Z}_m$. In [5], cyclic Hamilton cycles with $d = 1$ and $d = -1$ are both used. For this paper, all cyclic Hamilton cycles have $d = 1$.

Lemma 2.3 (from [5])**.** *If H is a cyclic Hamilton cycle of G with $d = 1$, then there exists a difference type $x \in \mathbb{Z}_m^{r-1}$ such that H is the union of all edges of the r difference types $\{x, x + e_1, \cdots, x + e_{r-1}\}$.*

Definition 2.4. The set of difference types given in Lemma 2.3 is called a *claw rooted at* x. Note that any claw of $\mathbb{Z}_m^{r-1}$ gives rise to a cyclic Hamilton cycle of $K^{(r)}_{r\times m}$.

Example 2.5. Let $r = 3$, $m = 4$, and $C = (0^0, 1^1, 3^2, 3^0, 0^1, 2^2, 2^0, 3^1, 1^2, 1^0, 2^1, 0^2, 0^0)$. This Hamilton cycle is cyclic by our definition. The difference types of C are $\{(1,2), (2,2), (1,3)\}$. This is the claw rooted at $(1,2)$. Furthermore, this claw admits the Hamilton cycle C.

Definition 2.6. A set $X \subseteq \mathbb{Z}_m^{r-1}$ is a *root set* if (a) $|X| = m^{r-1}/r$, and for every $x \in X$ both (b) $x + e_i \notin X$ for each $i \in [r-1]$ and (c) $x + e_i - e_j \notin X$ for all $\{i, j\} \subseteq [r-1]$ $(i < j)$.

Observe that condition (c) is equivalent to saying for all $\{x, x'\} \subseteq X$ and $\{i, j\} \subseteq [r-1]$, if $x + e_i = x' + e_j$, then $x = x'$ and $i = j$. Thus, if X is a root set of $\mathbb{Z}_m^{r-1}$, then $\mathcal{X} = \{\{x, x + e_1, \ldots, x + e_{r-1}\} : x \in X\}$ is a partition of $\mathbb{Z}_m^{r-1}$ into claws, and hence gives rise to a (cyclic) Hamilton cycle decomposition of $K^{(r)}_{r\times m}$. So one way to find a Hamilton cycle decomposition of $K^{(r)}_{r\times m}$ is to find a root set for $\mathbb{Z}_m^{r-1}$. To this end, we seek to prove the following:

Theorem 2.7. *Let $r \geq 2$ and $m \geq 2$ be positive integers. Then $\mathbb{Z}_m^{r-1}$ has a root set if and only if $r \mid m^{r-1}$.*

For a given r, let m_0 be the largest square-free integer dividing r. Then $r \mid m^{r-1}$ implies that $m_0 \mid m$. The following lemma shows that if $\mathbb{Z}_{m_0}^{r-1}$ has a root set, then so must $\mathbb{Z}_m^{r-1}$. From there on, we need only to show that $\mathbb{Z}_{m_0}^{r-1}$ has a root set, which is covered in Section 3.

Lemma 2.8. *Let r and m be positive integers with $r \geq 2$ and suppose $\mathbb{Z}_m^{r-1}$ has a root set. Then $\mathbb{Z}_{qm}^{r-1}$ also has a root set for any positive integer q.*

Proof. Let ϕ_m be the bijective map from $\mathbb{Z}_q \times \mathbb{Z}_m \to \mathbb{Z}_{qm}$ defined as $\phi_m(a,b) = m \cdot a + b$. This can be extended to a map from $\mathbb{Z}_q^{r-1} \times \mathbb{Z}_m^{r-1} \to \mathbb{Z}_{qm}^{r-1}$ component-wise. Observe that for any $a \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_m$, there exists $a' \in \mathbb{Z}_q$ such that $\phi_m(a,b) + 1 = \phi_m(a', b+1)$, (namely, $a' = a$ or $a+1$). Furthermore, for any $a \in \mathbb{Z}_q^{r-1}$, $b \in \mathbb{Z}_m^{r-1}$, and $\{i,j\} \subseteq [r-1]$ $(i < j)$, there exist $\{a', a''\} \subseteq \mathbb{Z}_q^{r-1}$ such that

$$\begin{aligned} \phi_m(a,b) + e_i &= \phi_m(a', b+e_i), \text{ and} \\ \phi_m(a,b) + e_i - e_j &= \phi_m(a'', b+e_i-e_j). \end{aligned}$$

Let X' be a root set of $\mathbb{Z}_m^{r-1}$. Define $X \subseteq \mathbb{Z}_{qm}^{r-1}$ as $X = \{\phi_m(u,x) : \ u \in \mathbb{Z}_q^{r-1}, \ x \in X'\}$. We now show that X is a root set:

(a) The cardinality of X is $(m^{r-1}/r) \cdot q^{r-1} = (qm)^{r-1}/r$.

(b) Assume that $x + e_i \in X$ for some $x \in X$ and $i \in [r-1]$. Then for some $\{u', u''\} \subseteq \mathbb{Z}_q^{r-1}$ and $\{x', x''\} \subseteq X'$, $x = \phi_m(u', x')$ and $x + e_i = \phi_m(u'', x'')$. So for some $u \in \mathbb{Z}_q^{r-1}$, $\phi_m(u'', x'') = x + e_i = \phi_m(u', x') + e_i = \phi_m(u, x' + e_i)$. Thus $\{x', x' + e_i\} \subseteq X'$, which contradicts X' being a root set.

(c) Assume that $x + e_i - e_j \in X$ for some $x \in X$, and $\{i,j\} \subseteq [r-1]$ $(i < j)$. Then for some $\{u', u''\} \subseteq \mathbb{Z}_q^{r-1}$ and $\{x', x''\} \subseteq X'$, $x = \phi_m(u', x')$ and $x + e_i - e_j = \phi_m(u'', x'')$. So for some $u \in \mathbb{Z}_q^{r-1}$, $\phi_m(u'', x'') = x + e_i - e_j = \phi_m(u', x') + e_i - e_j = \phi_m(u, x' + e_i - e_j)$. Thus $\{x', x' + e_i - e_j\} \subseteq X'$, contradicting X' being a root set. □

3 Constructions of Root Sets

We begin by describing the existence and properties of Hamming codes. See [8] for further information.

Let $p \geq 2$ be prime and let $t \geq 1$ be any positive integer. Let $n = (p^t - 1)/(p-1)$. Then there exists a subspace $X \subseteq \mathbb{Z}_p^n$ (a Hamming code) such that

- X is of dimension $n - t = (p^t - 1)/(p-1) - t$, and thus contains p^{n-t} vectors.
- X is a perfect 1-error correcting code, which means that for any vector $y \in \mathbb{Z}_p^n$, either $y \in X$ or there is a unique $x \in X$ for which the Hamming distance $d(x,y)$ (the number of non-agreeing components in their vectors) is 1. Furthermore, $d(x,x') \geq 3$ for all $\{x, x'\} \subseteq X$ $(x \neq x')$.

3.1 The $r = 2^k$ case

First, we look at the case when $m = 2$ and $r = 2^k$, i.e. we want a root set of $\mathbb{Z}_2^{2^k-1}$. From what we just established, we can find a Hamming code X with prime $p = 2$ and $t = k$. We claim that X is a root set. Observe that $n = 2^k - 1 = r - 1$ and X has dimension $n - t = 2^k - k - 1$, having $2^{2^k-k-1} = m^{r-1}/r$ vectors. We need only show properties (b) and (c) hold.

Let $x \in X$ and $\{i, j\} \subseteq [2^k - 1]$ $(i \neq j)$. Since the Hamming distances $d(x, x + e_i) = 1$ and $d(x, x + e_i - e_j) = 2$ and are each less than 3, $x + e_i \notin X$ and $x + e_i - e_j \notin X$.

Therefore, X is a root set of $\mathbb{Z}_2^{2^k-1}$.

3.2 The $r = p^k$ case

Let $m = p$ be any prime and $r = p^k$. Let $t = k$ and $n = (p^k - 1)/(p - 1)$. Let $z \in \mathbb{Z}_p^{(p-2)n}$. Define z_ϕ as the $(p - 2) \times n$ matrix obtained by reading the entries of z row by row. Let $z_\sigma \in \mathbb{Z}_p^n$ be the matrix product $z_\sigma = [1\ 2 \cdots\ p - 2] \cdot z_\phi$. See Example 3.1.

Observe that $(z + z')_\phi = z_\phi + z'_\phi$ and $(z + z')_\sigma = z_\sigma + z'_\sigma$ for any $z, z' \in \mathbb{Z}_p^{(p-2)n}$. Note that ϕ provides a 1-1 correspondence between the ordinates of z and the cells of z_ϕ. Let the ith ordinate of z correspond with the (r_i, c_i) cell in z_ϕ. Then $[e_i]_\sigma = r_i e_{c_i}$.

Example 3.1. Let $p = 5$ and $k = 2$, making $n = 6$. Let $z \in \mathbb{Z}_5^{18}$ be given as below.

$$z = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

Then z_ϕ and z_σ are

$$z_\phi = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \\ 2 & 3 & 4 & 0 & 1 & 2 \end{bmatrix} \quad \text{and} \quad z_\sigma = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \cdot z_\phi = \begin{bmatrix} 3 & 4 & 0 & 1 & 2 & 3 \end{bmatrix}.$$

If $i = 10$, then

$$[e_i]_\phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad [e_i]_\sigma = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \cdot [e_i]_\phi = \begin{bmatrix} 0 & 0 & 0 & 2 & 0 & 0 \end{bmatrix}.$$

Let $X \subseteq \mathbb{Z}_p^n$ be a Hamming code which has dimension $n - t = (p^k - 1)/(p - 1) - k$. From this set, we build a set $\overline{X} \subseteq \mathbb{Z}_p^{p^k-1}$ in the following way:

$$\overline{X} = \{(x + z_\sigma) \times z : x \in X \text{ and } z \in \mathbb{Z}_p^{(p-2)n}\}.$$

Lemma 3.2. *$\overline{X}$ is a root set.*

Proof. We need to show the three properties outlined in Definition 2.6.

(a) The cardinality of $\overline{X}$ is $p^{n-k} \times p^{n(p-2)} = p^{n(p-1)-k} = p^{p^k-1-k} = m^{r-1}/r$.

(b) Assume that $\overline{x} + e_i \in \overline{X}$ for some $\overline{x} \in \overline{X}$ and $i \in [r-1]$. Then $\overline{x} = (x + z_\sigma) \times z$ and $\overline{x} + e_i = (x' + z'_\sigma) \times z'$ for some $\{x, x'\} \subseteq X$ and $\{z, z'\} \subseteq \mathbb{Z}_p^{(p-2)n}$. So

$$(x + z_\sigma) \times z + e_i = (x' + z'_\sigma) \times z'.$$

First, suppose $i > n$. Then $z' = z + e_{i-n}$ and $x + z_\sigma = x' + z'_\sigma$. Let (r_i, c_i) be the cell of z_ϕ corresponding to the $(i-n)$ entry of z. Then $z_\sigma + r_i e_{c_i} = z'_\sigma$. Therefore,

$$x = x' + z'_\sigma - z_\sigma = x' + (z_\sigma + r_i e_{c_i}) - z_\sigma = x' + r_i e_{c_i}.$$

So $d(x, x') = 1$, which contradicts X being a Hamming code. Then $i \leq n$. So $z = z'$ (and hence $z_\sigma = z'_\sigma$) and $x + z_\sigma + e_i = x' + z'_\sigma$. Then $x + e_i = x'$, which gives that $d(x, x') = 1$, which again contradicts X being a Hamming code. Thus if $\overline{x} \in \overline{X}$, then $\overline{x} + e_i \notin \overline{X}$.

(c) Assume that $\overline{x} + e_i - e_j \in \overline{X}$ for some $\overline{x} \in \overline{X}$ and $\{i, j\} \subseteq [r-1]$ $(i < j)$. Then $\overline{x} = (x + z_\sigma) \times z$ and $\overline{x} + e_i - e_j = (x' + z'_\sigma) \times z'$ for some $\{x, x'\} \subseteq X$ and $\{z, z'\} \subseteq \mathbb{Z}_p^{(p-2)n}$. So

$$(x + z_\sigma) \times z + e_i - e_j = (x' + z'_\sigma) \times z'.$$

This argument is split into three cases:

Case 1. Suppose $n < i < j$. Then $x + z_\sigma = x' + z'_\sigma$ and $z + e_{i-n} - e_{j-n} = z'$. Let (r_i, c_i) and (r_j, c_j) be the cells in z_ϕ which correspond to the $(i-n)$ and $(j-n)$ entries of z, respectively. Then $z_\sigma + r_i e_{c_i} - r_j e_{c_j} = z'_\sigma$. Thus

$$x = x' + z'_\sigma - z_\sigma = x' + (z_\sigma + r_i e_{c_i} - r_j e_{c_j}) - z_\sigma = x' + r_i e_{c_i} - r_j e_{c_j}.$$

If $c_i = c_j$, then $r_i \neq r_j$, and $d(x, x') = 1$, which contradicts X being a Hamming code. If $c_i \neq c_j$, then $d(x, x') = 2$, which also contradicts X being a Hamming code.

Case 2. Suppose $i \leq n < j$. Then $x + z_\sigma + e_i = x' + z'_\sigma$ and $z - e_{j-n} = z'$. Let (r_j, c_j) be the cell of z_ϕ which corresponds to the $(j-n)$ entry of z. Then $z_\sigma - r_j e_{c_j} = z'_\sigma$. So

$$x = x' + z'_\sigma - z_\sigma - e_i = x' + (z_\sigma - r_j e_{c_j}) - z_\sigma - e_i = x' - r_j e_{c_j} - e_i.$$

If $c_j \neq i$, then $d(x, x') = 2$, which contradicts X being a Hamming code. Since $1 \leq r_j \leq p-2$, if $c_j = i$, then $d(x, x') = 1$, which also contradicts X being a Hamming code.

Case 3. Suppose $i < j \leq n$. Then $x + z_\sigma + e_i - e_j = x' + z'_\sigma$ and $z = z'$. Thus $z_\sigma = z'_\sigma$, which gives $x + e_i - e_j = x'$. Since $i \neq j$, we have $d(x, x') = 2$, which contradicts X being a Hamming code.

Therefore, $\overline{X}$ is a root set of $\mathbb{Z}_p^{p^k-1}$. □

3.3 The composite case

Let $r = PQ$ for relatively prime integers P and Q. Let p and q be the largest square-free integers dividing P and Q, respectively. Suppose $X'_p \subseteq \mathbb{Z}_p^{P-1}$ and $X'_q \subseteq \mathbb{Z}_q^{Q-1}$ are root sets. From these, we construct a root set of $\mathbb{Z}_{pq}^{PQ-1}$. Such a construction, coupled with Lemmas 3.2 and 2.8, proves Theorem 2.7 for any r and m for which $r \mid m^{r-1}$.

Let $z \in \mathbb{Z}_{pq}^{(P-1)(Q-1)}$. Define z_ϕ as the $(P-1) \times (Q-1)$ matrix whose entries are from z read in row by row. Let $z_\rho \in \mathbb{Z}_{pq}^{P-1}$ be the transpose of the row sum vector of z_ϕ. Let $z_\tau \in \mathbb{Z}_{pq}^{Q-1}$ be the column sum vector of z_ϕ. Observe that $(z+z')_a = z_a + z'_a$ when $a \in \{\phi, \rho, \tau\}$. Again, note that ϕ provides a 1-1 correspondence between the ordinates of z and the cells of z_ϕ. Let (r_i, c_i) denote the cell of z_ϕ corresponding with the ith ordinate of z. Then $(e_i)_\rho = e_{r_i}$ and $(e_i)_\tau = e_{c_i}$.

Example 3.3. Let $P = 4$ and $Q = 5$ (and hence $p = 2$ and $q = 5$). Let $z \in \mathbb{Z}_{10}^{12}$ be as given below.

$$z = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 \end{bmatrix}$$

Then z_ϕ, z_ρ, and z_τ are

$$z_\phi = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 0 & 1 \end{bmatrix}, \; z_\rho = \begin{bmatrix} 6 & 2 & 8 \end{bmatrix}, \text{ and } z_\sigma = \begin{bmatrix} 2 & 5 & 8 & 1 \end{bmatrix}.$$

Additionally,

$$[e_7]_\phi = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; [e_7]_\rho = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}, \text{ and } [e_7]_\sigma = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}.$$

By Lemma 2.8, there exist root sets $X_p \subseteq \mathbb{Z}_{pq}^{P-1}$ and $X_q \subseteq \mathbb{Z}_{pq}^{Q-1}$ constructed from X'_p and X'_q. Define $X \subseteq \mathbb{Z}_{pq}^{PQ-1}$ in the following manner:

$$X = \left\{ (x_p + z_\rho) \times (x_q + z_\tau) \times z \mid x_p \in X_p, \; x_q \in X_q, \; z \in \mathbb{Z}_{pq}^{(P-1)(Q-1)} \right\} \tag{2}$$

For sake of clarity, we denote the indices as

$$\begin{array}{rcll} \mathcal{P} & = & \{1, \ldots, P-1\} & \text{(the indices for } x_p + z_\rho\text{)} \\ \mathcal{Q} & = & \{P, \ldots, P+Q-2\} & \text{(the indices for } x_q + z_\tau\text{)} \\ \mathcal{R} & = & \{P+Q-1, \ldots, PQ-1\} & \text{(the indices for } z\text{)} \end{array}$$

Lemma 3.4. *X is a root set of $\mathbb{Z}_{pq}^{PQ-1}$.*

Proof. As with Lemma 3.2, we must show the three properties of Definition 2.6 hold.

(a) The cardinality of X is

$$\frac{(pq)^{P-1}}{P} \cdot \frac{(pq)^{Q-1}}{Q} \cdot (pq)^{(P-1)(Q-1)} = \frac{(pq)^{PQ-1}}{PQ} = \frac{m^{r-1}}{r}.$$

(b) Assume that $x + e_i \in X$ for some $x \in X$ and $i \in [PQ-1]$. Then

$$(x_p + z_\rho) \times (x_q + z_\tau) \times z + e_i = (x'_p + z'_\rho) \times (x'_q + z'_\tau) \times z'$$

for some $\{x_p, x'_p\} \subseteq X_p$, $\{x_q, x'_q\} \subseteq X_q$, and $\{z, z'\} \subseteq \mathbb{Z}_{pq}^{(P-1)(Q-1)}$.

If $i \in \mathcal{P}$, then $z = z'$ (and hence $z_\rho = z'_\rho$), giving $x_p + e_i = x'_p$, which contradicts X_p being a root set. If $i \in \mathcal{Q}$, again $z = z'$ (and hence $z_\tau = z'_\tau$), giving $x_q + e_j = x'_q$ (where $j = i - P + 1$), which contradicts X_q being a root set. If $i \in \mathcal{R}$, then $z + e_j = z'$ (where $j = i - (P + Q - 2)$). Let (r_j, c_j) be the cell of z_ϕ corresponding with the jth ordinate of z. So $z'_\rho = [z + e_j]_\rho = z_\rho + e_{r_j}$. Then

$$x_p = x'_p + z'_\rho - z_\rho = x'_p + (z_\rho + e_{r_j}) - z_\rho = x'_p + e_{r_j},$$

contradicting X_p being a root set. Thus, if $x \in X$, then $x + e_i \notin X$ for all $i \in [PQ-1]$.

(c) Assume that $x + e_i - e_j \in X$ for some $\{i, j\} \subseteq [PQ-1]$, $(i < j)$, and $x \in X$.

$$(x_p + z_\rho) \times (x_q + z_\tau) \times z + e_i - e_j = (x'_p + z'_\rho) \times (x'_q + z'_\tau) \times z'$$

for some $\{x_p, x'_p\} \subseteq X_p$, $\{x_q, x'_q\} \subseteq X_q$, and $\{z, z'\} \subseteq \mathbb{Z}_{pq}^{(P-1)(Q-1)}$. We will consider this in cases based on the location of the indices i and j.

Case 1. Suppose that $j \notin \mathcal{R}$ (and hence $i \notin \mathcal{R}$). Then $z = z'$, and thus $z_\rho = z'_\rho$ and $z_\tau = z'_\tau$. If $\{i, j\} \subseteq \mathcal{P}$, then $x_p + e_i - e_j = x'_p$, contradicting X_p being a root set. If $\{i, j\} \subseteq \mathcal{Q}$, then $x_q + e_{i'} - e_{j'} = x'_q$ (where $i' = i - P + 1$ and $j' = j - P + 1$), contradicting X_q being a root set. If $i \in \mathcal{P}$ and $j \in \mathcal{Q}$, then $x_p + e_i = x'_p$, contradicting X_p being a root set.

Case 2. Suppose that $j \in \mathcal{R}$ and $i \notin \mathcal{R}$. Then $z' = z + e_{j'}$ (where $j' = j - P - Q + 2$). Let (r_j, c_j) denote the cell of z_ϕ corresponding to the (j')th entry of z. If $i \in \mathcal{P}$, then $x'_q = x_q - e_{c_j}$, contradicting X_q being a root set. If $i \in \mathcal{Q}$, then $x'_p = x_p - e_{r_j}$, contradicting X_p being a root set.

Case 3. Suppose $\{i, j\} \subseteq \mathcal{R}$. Let $k = i - (P + Q - 2)$ and $l = j - (P + Q - 2)$, so $z + e_k - e_l = z'$. Then $z_\rho + e_{r_k} - e_{r_l} = z'_\rho$ and $z_\tau + e_{c_k} - e_{c_l} = z'_\tau$. Suppose $r_k \neq r_l$. Then

$$x_p = x'_p + z'_\rho - z_\rho = x'_p + (z_\rho + e_{r_k} - e_{r_l}) - z_\rho = x'_p + e_{r_k} - e_{r_l},$$

contradicting X_p being a root set. If $r_k = r_l$, then $c_k \neq c_l$, and thus

$$x_q = x'_q + z'_\tau - z_\tau = x'_q + (z_\tau + e_{c_k} - e_{c_l}) - z_\tau = x'_q + e_{c_k} - e_{c_l},$$

contradicting X_q being a root set. Therefore, if $x \in X$, then $x + e_i - e_j \notin X$. □

Combining the results of Lemmas 2.8, 3.2, and 3.4 give a proof of Theorem 2.7. Thus, we have the following result:

Theorem 3.5. *Let $m, r \geq 2$ be integers. Then $K^{(r)}_{r\times m}$ has a Hamilton cycle decomposition if and only if $r \mid m^{r-1}$.*

4 Previous Constructions

For the remainder of the paper, we say the root sets constructed in the previous sections are *code-constructed*. In [5], a root set is found for cases where r divides m, and is constructed differently.

Definition 4.1 (from [5])**.** Let $r \geq 2$ and $m \geq 2$ so that r divides m. For each $j \in \mathbb{Z}_r$, define $\mathcal{A}_j \subseteq \mathbb{Z}_m^{r-1}$ as

$$\mathcal{A}_j = \left\{ (x_1, \ldots, x_{r-1}) : \sum_{i=1}^{r-1} i x_i = j \pmod r \right\}$$

Suppose $x \in \mathcal{A}_0$. Then $x + e_i \in \mathcal{A}_i$ and $x + e_i - e_j \in \mathcal{A}_{i-j}$, for all pairs $\{i, j\} \subseteq \mathbb{Z}_r$. Therefore, $|\mathcal{A}_j| = m^{r-1}/r$ for each $j \in \mathbb{Z}_r$. Hence, $\mathcal{A}_0$ is a root set of $\mathbb{Z}_m^{r-1}$.

Definition 4.2. Let X be a root set of $\mathbb{Z}_m^{r-1}$. Then X is *satisfactory* if there exists an ordering $(a_1, \ldots, a_{r-1})$ of $[r-1]$ such that for each $x = (x_1, \ldots, x_{r-1}) \in X$,

$$\sum_{i=1}^{r-1} a_i x_i = 0 \pmod r. \tag{3}$$

Observe that $\mathcal{A}_0$ is a satisfactory root set, and any other satisfactory root set is isomorphic to $\mathcal{A}_0$ by permuting the ordinates. In [5], the constructions assumed that r divides m. We first show this is a necessary condition, and that a code-constructed set is satisfactory if, and only if, r is square-free. Note that when r is not square-free, the previous result in Section 3.2 gives rise to a code-constructed Hamilton cycle decomposition of $K^{(r)}_{r\times m}$ which is not isomorphic to the satisfactory Hamilton cycle decomposition found in [5].

Lemma 4.3. *Let r and m be integers and let $X \subseteq \mathbb{Z}_m^{r-1}$ be a satisfactory root set. Then r divides m.*

Proof. Without loss of generality, we assume that $X = \mathcal{A}_0$. Since r divides m^{r-1}, every prime dividing r also divides m. Since m and r have common factors, it follows that $m \neq 1 \bmod r$. Let $j = 1 - m \bmod r$, (so $j \neq 0$) and let $y = e_j - e_1 = e_j + (m-1)e_1$. So

$$\sum_{i=1}^{r-1} i y_i = j + (m-1) = 0 \bmod r. \tag{4}$$

So $y \in X$. Since $\{\vec{0}, y\} \subseteq X$ and $\vec{0} + e_j = y + e_1$, it follows that $j = 1$ and $y = \vec{0}$. So by (4), $m = 0 \bmod r$, giving that r divides m. □

Lemma 4.4. *Let r, m, and q be positive integers with $r \geq 2$ and r dividing m. Let X and $\overline{X}$ be the code-constructed sets of $\mathbb{Z}_m^{r-1}$ and $\mathbb{Z}_{qm}^{r-1}$, respectively. If X is satisfactory, then $\overline{X}$ is also satisfactory.*

Proof. Let $m = tr$ and let $(a_1, \ldots, a_{r-1})$ be an ordering of $[r-1]$ such that for each $x' \in X$,

$$\sum_{i=1}^{r-1} a_i x'_i = 0 \pmod{r}.$$

Let $x \in \overline{X}$. Then $x = x' + m \cdot u'$, where $x' \in X$ and $u' \in \mathbb{Z}_q^{r-1}$. So

$$\sum_{i=1}^{r-1} a_i x_i = \sum_{i=1}^{r-1} a_i (x'_i + m u'_i) = \sum_{i=1}^{r-1} a_i (x'_i + tr u'_i) = 0 \pmod{r}.$$

Therefore, $\overline{X}$ is satisfactory. □

Lemma 4.5. *Let r and m be integers such that $r \geq 2$ and r divides m. If $X \subseteq \mathbb{Z}_m^{r-1}$ is a satisfactory, code-constructed root set, then r is square-free.*

Proof. Let $(a_1, \ldots, a_{r-1})$ be a reordering of $[r-1]$ such that (3) holds for each $x \in X$. Let r' be the largest square-free integer dividing r and define t so that $r = tr'$. By the construction in Lemma 2.8, the code-constructed root set $X' \subseteq \mathbb{Z}_{r'}^{r-1}$ is embedded in X, and $x' + r'e_i \in X$ for each $i \in [r-1]$, $x' \in X'$, and $e_i \in \mathbb{Z}_m^{r-1}$. Let $x \in X'$ be fixed. Since $x' + r'e_i$ and x' each satisfy (3), then so must $r'e_i$. So $a_i r' = 0 \pmod{r}$, meaning that $a_i = b_i t$ for some $b_i \in [r'-1]$. It follows that for $a_1, \ldots, a_{r-1}$ to be distinct, $r = r'$. So r is squarefree. □

Proposition 4.6. *Let $X \subseteq \mathbb{Z}_p^{p-1}$ be a code-constructed root set. Then X is satisfactory.*

Proof. The code-constructed root set X with $m = p$, $r = p$, and $k = 1$ (and thus $n = 1$) involves the use of a trivial Hamming code of dimension 0, which is $\{0\} \subseteq \mathbb{Z}_p$. Let $x \in \overline{X}$. Then $x = z_\sigma \times z$, where $z \in \mathbb{Z}_p^{p-2}$. By its definition, z_σ is given by the sum

$$z_\sigma = \sum_{i=1}^{p-2} i z_i$$

Let $a_1 = p - 1$ and $a_i = (i-1)$ for each i, $2 \leq i \leq p-1$. Then

$$\sum_{i=1}^{p-1} a_i x_i = a_1 x_1 + \sum_{i=2}^{p-1} a_i x_i = (p-1) z_\sigma + \sum_{i=1}^{p-2} i z_i = p z_\sigma = 0 \pmod{p}$$

Thus, X is satisfactory. □

Proposition 4.7. *Let p and q be relatively prime integers and suppose the code-constructed root sets of $\mathbb{Z}_p^{p-1}$ and $\mathbb{Z}_q^{q-1}$ are satisfactory. Then the code-constructed root set of $\mathbb{Z}_{pq}^{pq-1}$ is satisfactory.*

Proof. Since the code-constructed root sets of $\mathbb{Z}_p^{p-1}$ and $\mathbb{Z}_q^{q-1}$ are satisfactory, by Lemma 4.4, so must the root sets $X_p \subseteq \mathbb{Z}_{pq}^{p-1}$ and $X_q \subseteq \mathbb{Z}_{pq}^{q-1}$. So there exist orderings $(a'_1, \ldots, a'_{p-1})$ and $(b'_1, \ldots, b'_{q-1})$ of $[p-1]$ and $[q-1]$ respectively so that for each $x_p \in X_p$ and $x_q \in X_q$,

$$\sum_{i=1}^{p-1} a'_i [x_p]_i = 0 \pmod{p} \quad \text{and} \quad \sum_{i=1}^{q-1} b'_i [x_q]_i = 0 \pmod{q}$$

Let X be the code-constructed root set as defined in (2) of Section 3.3. Let $x \in X$, where $x = (x + z_\rho) \times (x + z_\tau) \times z$ for some $x_p \in X_p$, $x_q \in X_q$, and $z \in \mathbb{Z}_{pq}^{(p-1)(q-1)}$. It is sufficient to show that there exists an ordering $(a_1, \ldots, a_{p-1}, b_1, \ldots, b_{q-1}, c_1, \ldots, c_{(p-1)(q-1)})$ of $[pq-1]$ such that

$$\sum_{i=1}^{p-1} a_i [x_p + z_\rho]_i + \sum_{i=1}^{q-1} b_i [x_q + z_\tau]_i + \sum_{i=1}^{(p-1)(q-1)} c_i z_i \tag{5}$$

is congruent to 0 (mod pq). Let $a_i = a'_i q$ and $b_j = b'_j p$ for each $i \in [p-1]$ and $j \in [q-1]$. So

$$\sum_{i=1}^{p-1} a_i [x_p]_i = 0 \pmod{pq} \quad \text{and} \quad \sum_{i=1}^{q-1} a_i [x_q]_i = 0 \pmod{pq}.$$

With our definitions of a_i and b_j, the expression in (5) reduces to

$$\sum_{i=1}^{p-1} a_i [z_\rho]_i + \sum_{i=1}^{q-1} b_i [z_\tau]_i + \sum_{i=1}^{(p-1)(q-1)} c_i z_i \pmod{pq}. \tag{6}$$

Let (r_i, k_i) be the corresponding cell in z_ϕ of the ith ordinate in z. Recall that $[e_i]_\rho = e_{r_i}$ and $[e_i]_\tau = e_{k_i}$. Let $\mathcal{R} = [(p-1)(q-1)]$. Observe that

$$[z_\rho]_i = \sum_{\substack{j \in \mathcal{R} \\ r_j = i}} z_j \text{ and } [z_\tau]_i = \sum_{\substack{j \in \mathcal{R} \\ k_j = i}} z_j.$$

For each $i \in \mathcal{R}$, define $c_i \in \mathbb{Z}_{pq}$ so $c_i = -a_{r_i} \pmod{p}$ and $c_i = -b_{k_i} \pmod{q}$. Observe that $c_i \neq 0$ modulo p or q, and hence $c_i \notin \{a_1, \ldots, a_{p-1}, b_1, \ldots, b_{q-1}\}$. Since (r_i, k_i) is distinct for each i, each c_i is distinct. So $(a_1, \ldots, a_{p-1}, b_1, \ldots, b_{q-1}, c_1, \ldots, c_{(p-1)(q-1)})$ is an ordering of $[pq-1]$. Now, we show that the expression in (5) is congruent to 0 modulo pq. First, we look at the expression in (6) modulo p:

$$\begin{aligned}
\sum_{i=1}^{p-1} a_i [z_\rho]_i + \sum_{j=1}^{(p-1)(q-1)} c_j z_j &= \sum_{i=1}^{p-1} a_i [z_\rho]_i + \sum_{j=1}^{(p-1)(q-1)} (-a_{r_j}) z_j &= \sum_{i=1}^{p-1} a_i [z_\rho]_i + \sum_{i=1}^{p-1} \sum_{\substack{j \in \mathcal{R} \\ r_j = i}} (-a_i) z_j \\
&= \sum_{i=1}^{p-1} a_i [z_\rho]_i - \sum_{i=1}^{p-1} a_i \sum_{\substack{j \in \mathcal{R} \\ r_j = i}} z_j &= \sum_{i=1}^{p-1} a_i [z_\rho]_i - \sum_{i=1}^{p-1} a_i [z_\rho]_i = 0.
\end{aligned}$$

Similarly, when looking at the expression in (6) modulo q:

$$\begin{aligned}\sum_{i=1}^{q-1} b_i[z_\tau]_i + \sum_{j=1}^{(p-1)(q-1)} c_j z_j &= \sum_{i=1}^{q-1} b_i[z_\tau]_i + \sum_{j=1}^{(p-1)(q-1)} (-b_{k_j}) z_j &= \sum_{i=1}^{q-1} b_i[z_\tau]_i + \sum_{i=1}^{q-1} \sum_{\substack{j\in\mathcal{R}\\ k_j=i}} (-b_i) z_j \\ &= \sum_{i=1}^{q-1} b_i[z_\tau]_i - \sum_{i=1}^{q-1} b_i \sum_{\substack{j\in\mathcal{R}\\ k_j=i}} z_j &= \sum_{i=1}^{q-1} b_i[z_\tau]_i - \sum_{i=1}^{q-1} b_i[z_\tau]_i = 0.\end{aligned}$$

Since the expression in (6) is congruent to 0 modulo p and q, the expression in (5) is congruent to 0 modulo pq, proving the proposition. □

The results of this section are summarized as follows:

Theorem 4.8. *Let r and m be positive integers with $r \geq 2$ and r dividing m^{r-1}. Then $\mathbb{Z}_m^{r-1}$ has a satisfactory root set if and only if r divides m. In this case, the code-constructed root set of $\mathbb{Z}_m^{r-1}$ is satisfactory if and only if r is square-free.*

References

[1] R. F. Bailey and B. Stevens, *Hamiltonian decompositions of complete k-uniform hypergraphs*, Discrete Math., 310 (2010), pp. 3088–3095.

[2] C. Berge, *Graphes et hypergraphes*, Dunod, Paris, 1970. Monographies Universitaires de Mathématiques, No. 37.

[3] J. L. Gross and J. Yellen, eds., *Handbook of graph theory*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, 2004.

[4] G. Y. Katona and H. A. Kierstead, *Hamiltonian chains in hypergraphs*, J. Graph Theory, 30 (1999), pp. 205–212.

[5] J. Kuhl and M. W. Schroeder, *Hamilton cycle decompositions of k-uniform k-partite hypergraphs*, Australas. J. Combin. To appear.

[6] E. Lucas, Récreations Mathématiqués, I-IV (1882–3, 1893–4).

[7] M. Meszka and A. Rosa, *Decomposing complete 3-uniform hypergraphs into Hamiltonian cycles*, Australas. J. Combin., 45 (2009), pp. 291–302.

[8] V. S. Pless, W. C. Huffman, and R. A. Brualdi, eds., *Handbook of coding theory. Vol. I, II*, North-Holland, Amsterdam, 1998.

[9] H. Verrall, *Hamilton decompositions of complete 3-uniform hypergraphs*, Discrete Math., 132 (1994), pp. 333–348.