Odd order 2(n+1) regular connected Cayley graphs on rank *n* elementary abelian groups are Hamilton decomposable

Cafer Caliskan, Donald L. Kreher
Michigan technological university

August 29, 2011

Abstract

First it is shown that every odd order $2(n+1)$-regular connected Cayley graph on an rank n elementary abelian group is Hamilton decomposable. We apply this result to Paley graphs and show that when given a odd prime power $q = p^n$, and even order rank n multiplicative subgroup S of the finite field $\mathbb{F}_q$, that the Cayley graph with connection set S is Hamilton decomposable, whenever $|S| \geq 2n^2$. This extends the recent result of Alspach, Bryant and Dyer on Paley graphs.

1 Introduction

Let A be an Abelian group and $S \subset A$ such that $0 \notin S$. We denote by $S^\star$ the inverse-closure of S, that is, $S^\star$ is the smallest superset of S satisfying $s \in S^\star$ if and only if $-s \in S^\star$.

The *Cayley graph* $\textsc{Cay}(A; S^\star)$ is the graph whose vertices are the elements of A with x adjacent to y if and only if $x - y \in S^\star$. The subset $S \subseteq A$ is called the *connection set* for the *Cayley graph* $\textsc{Cay}(A; S^\star)$ and an edge $\{x, y\}$ of $\textsc{Cay}(A; S^\star)$ is an s-edge if $x \pm s = y$, for $s \in S$.

A cycle that spans the vertices of a graph X is called a *Hamilton cycle* of X. A *Hamilton decomposition* of a regular graph with even valence is a partition of its edge set into Hamilton cycles. A *Hamilton decomposition* of a regular graph with odd valence is a partition of its edge set into Hamilton cycles and a single one-factor. A graph admitting a Hamilton decomposition is said to be *Hamilton-decomposable*. See Figures 1 and 2. Alspach [1] conjectured in 1984, that Cayley graphs on Abelian groups are Hamilton-decomposable. This conjecture remains unresolved. Bermond [3] conjectured in 1978, that Cartesian product of Hamilton-decomposable graphs is Hamilton-decomposable. This conjecture also remains unresolved, but there is a very useful partial result due to Stong [6]. Stong's result includes the following theorem which we require.

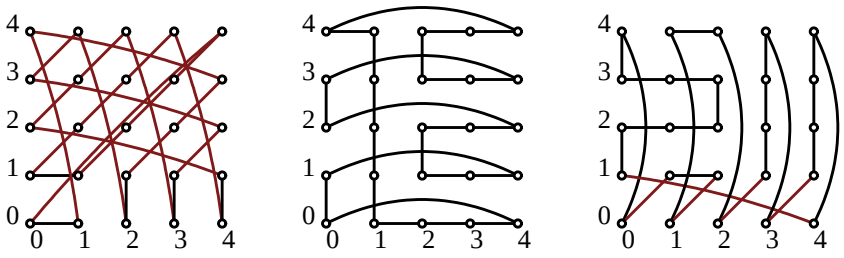


Figure 1: A Hamilton decomposition of $\textsc{Cay}(\mathbb{Z}_5^2; \{(1,1),(0,1),(1,0)\}^\star)$

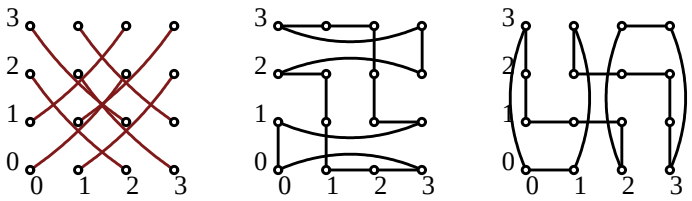


Figure 2: A Hamilton decomposition of $\textsc{Cay}(\mathbb{Z}_4^2; \{(2,2),(0,1),(1,0)\}^\star)$

Theorem 1.1 (Stong 1991) *If X_1 is a Hamilton-decomposable graph of valency $2r$ and X_2 is a Hamilton-decomposable graph of valency $2s$, with $r \leq s$, then the Cartesian product $X_1 \square X_2$ is Hamilton-decomposable if either of the following two conditions holds:*

1. *$s \leq 3r$, or*
2. *$r \geq 3$.*

According to [2] the proof of the next theorem was not given completely in the original paper [4] because "they interpreted involutions in an unusual way". It is also asserted in [2] that completing their proof is a trivial exercise.

Theorem 1.2 (Bermond, Favaron, Meheao 1989 and Alspach, Bryant, Dyer 2010) *Every connected Cayley graph of valency 4 on an Abelian group is Hamilton-decomposable.*

For graphs of valency 6, a result was recently obtained by Westlund, Liu and Kreher [7].

Theorem 1.3 (Westlund, Kreher and Liu 2009) *Every connected Cayley graph of valency 6 on an odd order Abelian group is Hamilton-decomposable.*

A corollary to these results obtained in [2] is

Corollary 1.4 *The cartesian product of any number of cycles and any number of connected Cayley graphs of valency 4 on Abelian groups is Hamilton-decomposable.*

The most important result that we establish in this article is

Theorem 1.5 (The Key) *Let S be a basis of $V = \mathbb{Z}_p^n$, p an odd prime, and let g be any non-zero vector of $V \setminus S$. Then the Cayley graph $X = \textsc{Cay}(V; (S \cup \{g\})^\star)$ has a Hamilton decomposition.*

Its proof which we provide in Section 3 is an induction proof that begins in dimension 2. We dedicate Section 2 to the $n = 2$ case. In Section 4 is our application of this Key Theorem to Paley graphs.

We end this section by reminding the reader of two fundamental techniques used in the construction of Hamilton decompositions, see for example [5]. If A and B are graphs on the vertex set V, then the *symmetric difference* of A and B is the graph $A \triangle B$ on V with edge set $(E(A) \setminus E(B)) \cup (E(B) \setminus E(A)$ the symmetric difference of the edge sets of A and B.

Technique 1: If $A_0, A_1, A_2, \ldots, A_{k-1}$ are pairwise edge-disjoint cycles and $C = x_0y_0x_1y_1x_2y_2 \cdots x_{k-1}y_{k-1}$ is a length $2k$ closed trail (for example a cycle) such that $x_iy_i \in E(A_0+A_1+\cdots+A_{k-1})$ for all i, but $y_ix_{i+1} \notin E(A_0+A_1+\cdots+A_{k-1})$ for any i (subscripts modulo k), then the symmetric difference

$$(A_0 + A_1 + \cdots + A_{k-1}) \triangle C$$

is a single cycle.

Technique 2: If A is a cycle of length ℓ with orientation $x_0x_1 \cdots x_\ell$ and F is a 4-cycle $abcd$ such that $\{a,b\},\{c,d\} \in E(A)$, $\{b,c\},\{a,d\} \notin E(A)$, and (a,b), (c,d) both agree with the orientation given to A, then the symmetric difference $A \triangle C$ is a cycle of length ℓ.

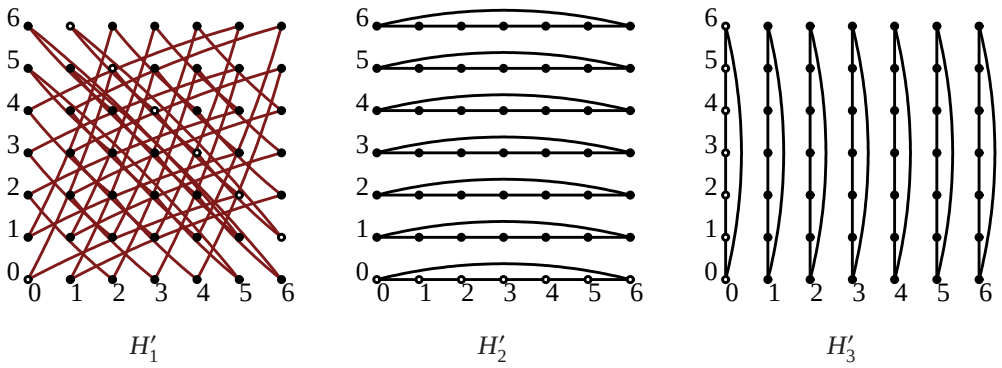


Figure 3: $\textsc{Cay}(\mathbb{Z}_7^2; \{(2,5),(0,1),(1,0)\}^\star)$

2 Dimension 2

Let p be an odd prime and let $\vec{r} = (a,b) \in \mathbb{Z}_p^2$, where neither a nor b is zero, also set $\vec{e}_1 = (1,0)$, $\vec{e}_2 = (0,1)$. In this section we consider the Cayley graph

$$X = \textsc{Cay}(\mathbb{Z}_p^2; \{\vec{r}, \vec{e}_1, \vec{e}_2\}^\star).$$

In this section we construct Hamilton decomposition H_1, H_2, H_3 of X where the subgraph R of $\vec{r}$-edges are distributed in one of 3 ways.

$$\mathbb{D}_1 := \begin{cases} H_1 \cap R, \text{ a set of } p \text{ disjoint paths and no isolated vertices.} \\ H_2 \cap R, \text{ a set of } p^2 \text{ isolated vertices.} \\ H_3 \cap R, \text{ a } p\text{-matching and } p^2 - 2p \text{ isolated vertices.} \end{cases}$$

$$\mathbb{D}_2 := \begin{cases} H_1 \cap R, \text{ a set of } p \text{ disjoint paths and 2 isolated vertices.} \\ H_2 \cap R, \text{ a set of } p^2 \text{ isolated vertices.} \\ H_3 \cap R, \text{ a } (p+2)\text{-matching and } p^2 - 2(p+2) \text{ isolated vertices.} \end{cases}$$

$$\mathbb{D}_3 := \begin{cases} H_1 \cap R, \text{ a set of } p+2 \text{ disjoint paths and 0 isolated vertices.} \\ H_2 \cap R, \text{ a set of } p^2 \text{ isolated vertices.} \\ H_3 \cap R, \text{ a } (p+2)\text{-matching and } p^2 - 2(p+2) \text{ isolated vertices.} \end{cases}$$

The existence of the Hamilton decomposition of X guaranteed by Theorem 1.3 need not yield a decomposition with the above desired distribution of $\vec{r}$-edges. To begin we start with the edge partition

$$H_1' = R, \qquad H_2' = \textsc{Cay}(\mathbb{Z}_p^2; \{\vec{e}_1\}^\star), \qquad H_3' = \textsc{Cay}(\mathbb{Z}_p^2; \{\vec{e}_2\}^\star).$$

An example when $p = 7$ is given in Figure 3. Let C be the cycle defined by the length $2p$ alternating $r,-\vec{e}_2$ sequence

$$(w_1, w_2, \ldots, w_{2p}) = (\vec{r}, -\vec{e}_2, \vec{r}, -\vec{e}_2, \ldots, \vec{r}, -\vec{e}_2)$$

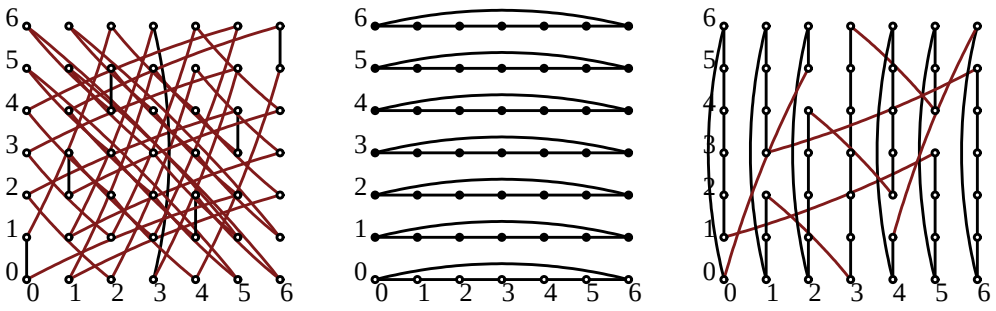
and the vertex $(0,0)$. That is

$$C = \left((0,0) + \sum_{i=1}^{j} w_i : j = 0, 1, 2, \ldots, 2p-1 \right).$$

This is a cycle because $\vec{r}$ and $\vec{e}_2$ are linearly independent. The edges of C alternate between edges of H_1' and H_3'. The $\vec{r}$-edges of C join the cycles of H_3' and the $\vec{e}_2$-edges of C join the cycles of H_1'. Thus the symmetric differences $H_1' \triangle C$ and $H_3' \triangle C$ are Hamilton cycles. See Figure 4. It is not difficult to see that the $\vec{e}_2$-edges used in the cycle C are

$$S = \{(ka, -k(1-b)), (ka, 1-k(1-b))\},$$

where $k = 0, 1, 2, \ldots, p-1$. There are two cases to consider.



$H_1' \triangle C$ | H_2' | $H_3' \triangle C$

A Hamilton cycle | p p-cycles | A Hamilton cycle

$$C = (0,0)(2,5)(2,4)(4,2)(4,1)(6,6)(6,5)(1,3)(1,2)(3,0)(3,6)(5,4)(5,3)(0,1)$$

Figure 4: Symmetric difference with the cycle C

Case 1 $b \neq 1$: Setting $x = ka$ and $z = -(b-1)^{-1}a$ we find the $\vec{e}_2$-edges used in the cycle C are:

$$S = \left\{\{(x, -z^{-1}x), (x, 1 - z^{-1}x)\} : x \in \mathbb{Z}_p\right\}$$

If the edge $s_x = \{(x, y_1), (x, y_2)\} \in S$, and $y_2 = y_1 + 1$ then we call y_2 the *top* of s and y_1 the *bottom* of s; otherwise y_1 is the top and y_2 is the bottom. Let $F_{\vec{x}}$, where $\vec{x} \in \mathbb{Z}_p^2$ be the 4-cycle defined by the sequence $(\vec{e}_1, \vec{e}_2, -\vec{e}_1, -\vec{e}_2)$ and the vertex $\vec{x}$ that is $F_{\vec{x}}$ is the subgraph with edge set

$$E(F_{\vec{x}}) = \{\{\vec{x}, \vec{x} + \vec{e}_1\}, \{\vec{x} + \vec{e}_1, \vec{x} + \vec{e}_1 + \vec{e}_2\}, \{\vec{x} + \vec{e}_1 + \vec{e}_2, \vec{x} + \vec{e}_2\}, \{\vec{x} + \vec{e}_2, \vec{x}\}\} .$$

Then focusing on $s_z = \{(z, -1), (z, 0)\}$ we define the *zig-zag* to be

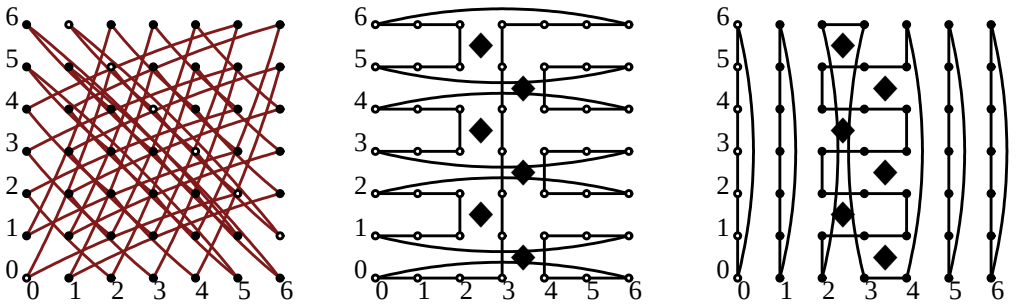
$$Z = \begin{cases} F_{(z-1,0)} + F_{(z,1)} + F_{(z-1,2)} + F_{(z,3)} + \cdots + F_{(z-1,p-2)} & \text{if } [z^{-1}] \text{ is odd;} \\ F_{(z+1,0)} + F_{(z,1)} + F_{(z+1,2)} + F_{(z,3)} + \cdots + F_{(z+1,p-2)} & \text{if } [z^{-1}] \text{ is even,} \end{cases}$$

where $[z^{-1}]$ is the unique integer such that $0 \leq [z^{-1}] < p$ and $[z^{-1}] \equiv z^{-1} \pmod{p}$. It should be observed that $S \cap E(Z) = \emptyset$. The zig-zag Z is a length $4(p-1)$ closed trail with edges alternating between H_2' and H_3'. Thus applying Technique 1 we find that the $\vec{e}_2$-edges of Z join the cycles of H_2' and consequently the symmetric difference $H_2' \triangle Z$ is a Hamilton cycle. The $\vec{e}_1$-edges of Z span only the cycles of H_3' that have first coordinate among $z-1$, z and $z+1$, thus these cycles are joined into a cycle of length $3p$ in the symmetric difference $H_3' \triangle Z$. The remaining vertices are in cycles of length p. An example when $p = 7$ is given in Figure 5. Consequently the symmetric differences $H_1' \triangle C$ and $H_2' \triangle Z$ are Hamilton cycles whereas $H_3' \triangle (C + Z)$ may not be. See Figure 6.

We now show that $H_3' \triangle (C + Z)$ is either a Hamilton cycle or consists of exactly two edge-disjoint cycles. The $3p$-cycle of $\vec{e}_1$- and $\vec{e}_2$-edges formed by the symmetric difference $H_3' \triangle Z$ is broken into three paths when the edges s_{z-1}, s_z and s_{z+1} are removed by the symmetric difference $H_3' \triangle (C + Z)$. These three paths of $\vec{e}_1$- and $\vec{e}_2$-edges are

- a top of s_{z-1} to the top of s_z path P_1
- a bottom of s_{z-1} to the top of s_{z+1} path P_2
- a bottom of s_{z-1} to the bottom of s_{z+1} path P_2

Each $\vec{r}$-edges in $H_3' \triangle (C + Z)$ is adjacent to exactly two edges in S; it is incident to one at the bottom end and another at the top end. When traversing the cycle containing an $\vec{r}$-edge $\{(x - a, y_2 - b), (x, y_2)\}$, where

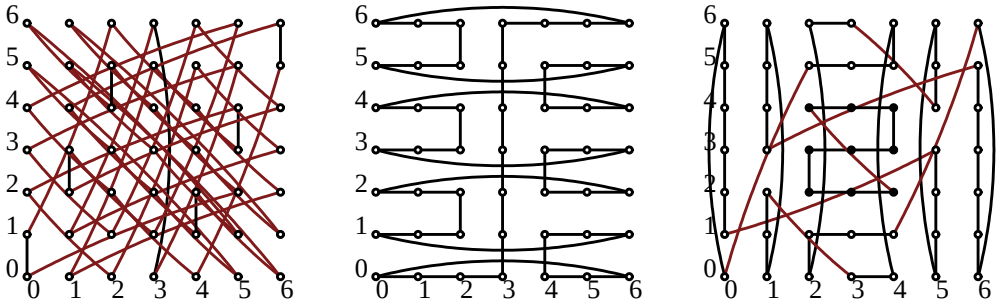


H'_1 | $H'_2 \triangle Z$ | $H'_3 \triangle Z$

p p-cycles | A Hamilton cycle | $p-3$ p-cycles and one $3p$-cycle

$$Z = F(3,0) + F(2,1) + F(3,2) + F(2,3) + F(3,4) + F(2,5)$$

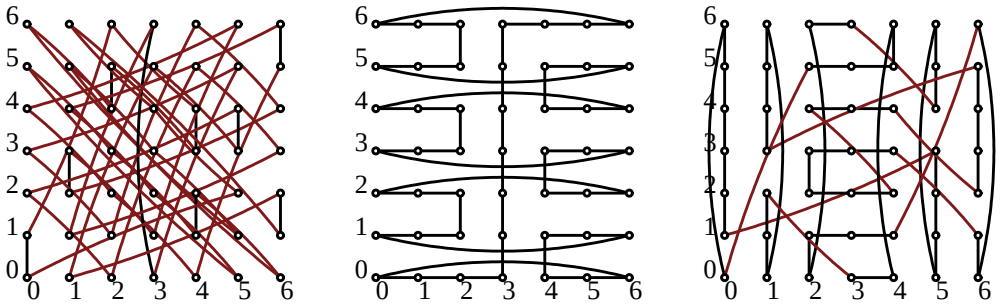
Figure 5: Symmetric difference with zig-zag Z marked with ◆.



$H'_1 \triangle C$ | $H'_2 \triangle Z$ | $H'_3 \triangle (C + Z)$

A Hamilton cycle | A Hamilton cycle | Two cycles

Figure 6: Symmetric difference with C and Z



$H_1 = H'_1 \triangle (C + D)$ | $H_2 = H'_2 \triangle Z$ | $H_3 = H'_3 \triangle (C + Z + D)$

A Hamilton cycle | A Hamilton cycle | A Hamilton cycle

Figure 7: Symmetric difference with C, Z, and $D = (4,3)(4,4)(6,2)(6,1)$

$x \notin \{z-1, z, z+1\}$ then it follows the path

$$(x, y_2+1)(x, y_2+2)\cdots(x, y_2+k)\cdots(x, y_2-1)$$

and then exits on the $\vec{r}$-edge $\{(x, y_2-1), (x+a, y_2-1+a)\}$. Hence it enters at the top of s_x and leaves at the bottom of s_x. It follows that the cycles containing P_1, P_2 or P_3 must join their top ends to bottom ends. Hence because P_1 has two top ends, P_2 has a top and bottom end and P_3 has two bottom ends, then we can only complete the traversal of cycles by either

1. joining P_1 and P_3 with intermediate edges into a cycle and simultaneously joining P_3 with intermediate edges into a cycle, thus obtaining two cycles.
2. joining P_1, P_2, P_3 with intermediate edges into a single cycle .

In the second case as mentioned earlier the graph X has been successfully decomposed into Hamilton cycles, and the decomposition has distribution $\mathbb{D}_1$. In the first case let K_1 and K_2 be the two cycles. Then because vertices with first coordinate x are joined by an $\vec{r}$-edge to vertices with first a coordinate $x+a$, there must exist without loss an $x \in \mathbb{Z}_p \setminus \{z\}$ where all of the edges $\{(x+a, i), (x+a, i+1)\}$ are edges of K_2 except the edge s_{x+a} and an edge $\{(x, y), (x, y+1)\}$ in K_1 where $\{(x+a, y), (x+a, y+1)\} \neq s_{x+a}$. Let D be the 4-cycle

$$(x, y)(x, y+1)(x+a, y+1+b)(x+a, y+b)$$

The edges of D alternate between $H_1' \triangle C$ and $K_1 + K_2 = H_3' \triangle (C+Z)$. Also when the edges of the Hamilton cycle $H_1' \triangle C$ are traversed, parallel edges are traversed in the same direction. Consequently, applying Technique 2, we see that $H_1' \triangle (C+D)$ and $H_3' \triangle (C+Z+D)$ are Hamilton cycles. This decomposition will have distribution $\mathbb{D}_2$ or $\mathbb{D}_3$ depending whether the edge $\{(x, y), (x+a, y+b)\}$ is at the end of a path in $(H_1' \triangle (C+D)) \cap R$ or in the middle of such a path. See Figure 7.

Case 2, $b = 1$: In this case the $\vec{e}_2$-edges used in the cycle C are:

$$S = \left\{\{(x, 0), (x, 1)\} : x \in \mathbb{Z}_p\right\}.$$

Similar to Case 1 we employ the zig-zag

$$Z = F_{(0,0)} + F_{(1,1)} + F_{(0,2)} + F_{(1,3)} + \cdots + F_{(0,p-2)}.$$

Only the 4-cycle $F(0, 0)$ has non-empty intersection with S. Thus $F(0, 0)$ alternates edges between $H_1' \triangle C$ and H_2', whereas the edges of the other 4-cycles in Z alternate between H_2' and $H_3' \triangle C$. The $\vec{e}_2$-edges of Z join the cycles of H_2' and thus $H_2 = H_2' \triangle Z$ is a Hamilton cycle. Thus because parallel $\vec{e}_2$-edges of $H_3' \triangle Z$ have the same orientation it follows that $H_3 = H_3' \triangle (Z - F(0, 0))$ is a Hamilton cycle. Also the edges $\{(0, 0), (0, 1)\}$ and $\{(1, 0), (1, 1)\}$ have the same orientation in $H_1' \triangle C$ so it follows that $H_1 = H_1' \triangle (C + F(0, 0))$ is a Hamilton cycle. This decomposition has $(a, 1)$-edge distribution $\mathbb{D}_1$. An example is provided in Figure 7.

We summarize with the following theorem:

Theorem 2.1 *For every odd prime p and non-zero elements a and b in $\mathbb{Z}_p$ the Cayley graph*

$$\textsc{Cay}(\mathbb{Z}_p^2; \{(a, b), (1, 0), (0, 1)\}^\star)$$

has a decomposition into Hamilton cycles H_1, H_2, H_3 with (a, b)-edge distribution either $\mathbb{D}_1$, $\mathbb{D}_2$ or $\mathbb{D}_3$.

3 Proof of the Key Theorem

Consider the finite vector space $V = \mathbb{Z}_p^n$ for some prime p and positive integer n. The automorphism group of V is $\mathrm{GL}_n(p)$ the group of n by n invertible matrices on $\mathbb{Z}_p$.

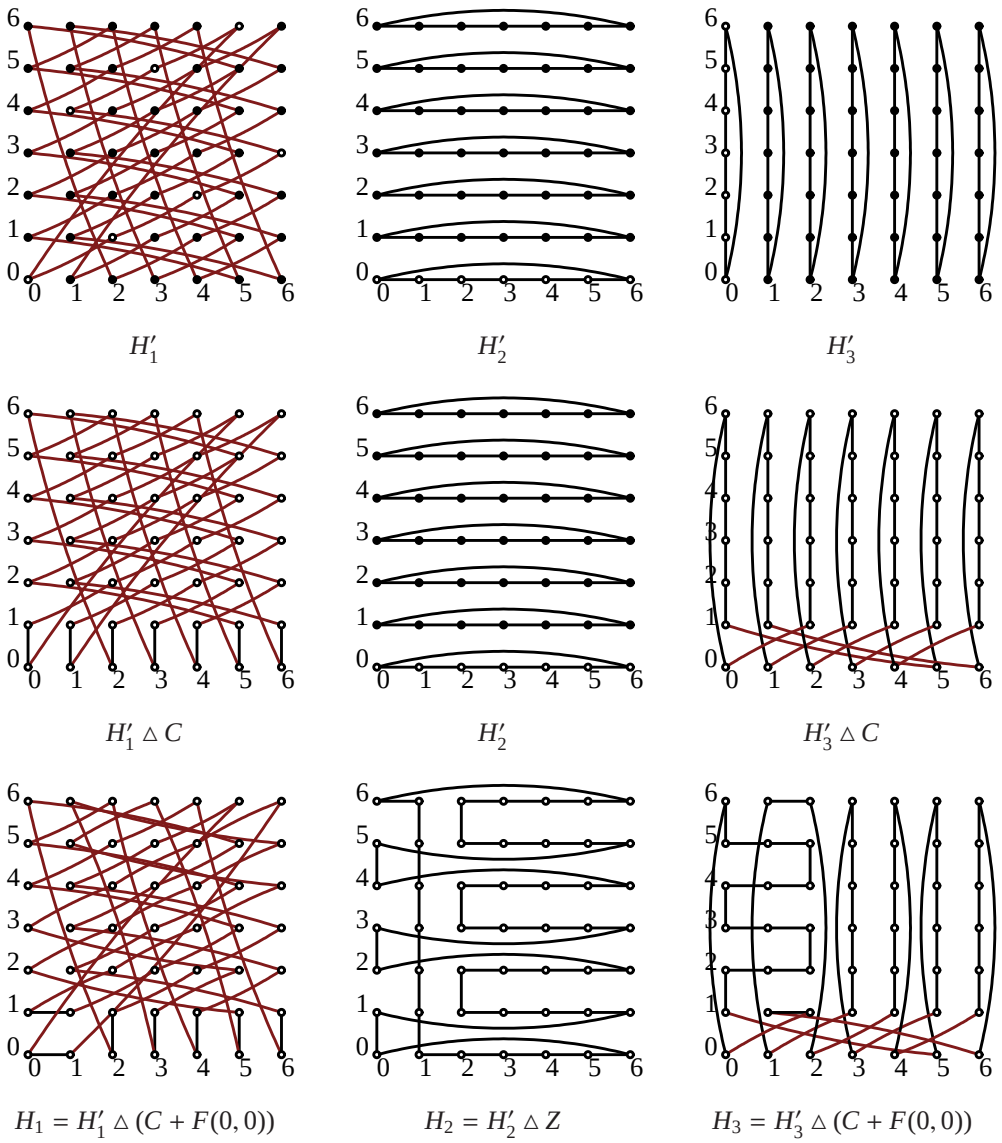


Figure 8: $\textsc{Cay}(Z_7^2; \{(2,1),(1,0),(0,1)\}^\star)$.

If $M \in \mathrm{GL}_n(p)$, then it is easy to see the mapping $x \mapsto Mx$ on V is a graph isomorphism from $\textsc{Cay}(V; S^\star)$ to $\textsc{Cay}(V; MS^\star)$. In particular if S is a linearly independent subset of V, then the matrix M whose columns are the elements of S is invertible and hence $M \in \mathrm{GL}_n(p)$. It follows that $\textsc{Cay}(V; S^\star)$ is isomorphic $\textsc{Cay}(V; \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}^\star)$, where $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ is the standard basis for V. That is

$$\vec{e}_j = [0, 0, \ldots, 0, \underbrace{1}_{j\text{-th}}, 0, \ldots, 0]$$

It is not difficult to prove the following:

Lemma 3.1 *If A and B are subsets of the finite dimensional vector space V that are orthogonal to each other, then*

$$\textsc{Cay}(\textsc{Span}\,(A \cup B)\,; A^\star \cup B^\star) \approx \textsc{Cay}(\textsc{Span}\,(A)\,; A^\star) \square \textsc{Cay}(\textsc{Span}\,(B)\,; B^\star)$$

An immediate consequence is Lemma 3.2 which appears in [2].

Lemma 3.2 (Alspach, Bryant, Dyer 2010) *If $S = \{s_1, s_2, \ldots, s_t\}$ is a set of linearly independent vectors in V, then the components of the Cayley graph $\textsc{Cay}(V; S^\star)$ are all isomorphic to the Cartesian product of t p-cycles.*

It has an interesting Corollary which also appears in [2].

Corollary 3.3 (Alspach, Bryant, Dyer 2010) *If S is a basis of $V = \mathbb{Z}_p^n$, then the Cayley graph $\textsc{Cay}(V; S^\star)$ has a Hamilton decomposition.*

Theorem 1.5 is our extension of this corollary and is key to the Sub-Paley graph Hamilton decomposition problem. Before proceeding to the proof of Theorem 1.5 we require some discussion and technical lemmas. If $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_p^n$, then for $k < n$ we denote by $\pi_k(\vec{x})$ the projection of $\vec{x}$ on to the first k coordinates. That is

$$\pi_k(\vec{x}) = (x_1, x_2, x_3, \ldots, x_k) \in \mathbb{Z}_p^k.$$

For ease of notation when $k > \ell$, we identify $\vec{e}_\ell$ with $\pi_k(\vec{e}_\ell)$. Let $S_k = \{\pi_k(\vec{r}), \vec{e}_1, \vec{e}_2, \ldots, \vec{e}_k\}$, where $\vec{r} \in \mathbb{Z}_p^n$ has no zero entry, and set

$$X_k = \textsc{Cay}(\mathbb{Z}_p^k; {S_k}^\star),$$

for $k = 1, 2, \ldots, n$. If H is any subgraph of X_k, we denote by $\mathrm{c}_{\overline{R}}(H)$ the number of connected components of $H - R_k$, where $R_k = \textsc{Cay}(\mathbb{Z}_p^k; \pi_k(\vec{r})^\star)$. Two edges $f_1 = \{\vec{x}_1, \vec{y}_1\}$ and $f_2 = \{\vec{x}_2, \vec{y}_2\}$ will be called *parallel* edges in X_k if

$$f_1 + \vec{e}_k = \{\vec{x}_1 + \vec{e}_k, \vec{y}_1 + \vec{e}_k\} = f_2,$$

for some e_k. A *special Hamilton decomposition* of X_k is a Hamilton decomposition $H_0, H_1, H_2, \ldots, H_k$, where $\mathrm{c}_{\overline{R}}(H_i) \leq p^k - (i+1)(p-1)$, for all i. Theorem 2.1 provides a special Hamilton decomposition of X_2.

If H is a subgraph of X_{k-1}, then the *lift* of H is that subgraph L of X_k, where

$$\{\vec{u}, \vec{v}\} \in E(L) \text{ if and only if } \{\pi_{k-1}(\vec{u}), \pi_{k-1}(\vec{v})\} \in E(H).$$

Lemma 3.4 *X_k has a special Hamilton decomposition, for all $k \geq 2$.*

Proof. We proceed by induction on k. If $k = 2$, then a special Hamilton decomposition is provided by Theorem 2.1. So suppose $k > 2$. Then by induction X_{k-1} has a special Hamilton-decomposition $H_0, H_1, H_2, \ldots, H_{k-1}$. Let L_i be the lift of H_i, $i = 0, 1, 2, \ldots, k-1$. Then

$$L_0, L_1, L_2, \ldots, L_{k-1}, G,$$

where $G = \textsc{Cay}(\mathbb{Z}_p^k; \vec{e}_k)$ is an edge decomposition of X_k. Because $H_0 - R$ has $\mathrm{c}_{\overline{R}}(H_0) \leq p^{k-1} - (p-1)$ components, it contains an acyclic subgraph S_0 with at least $p^{k-1} - (p^{k-1} - (p-1)) = (p-1)$ edges.

Suppose $t < k$ and for $0 \le i < t$ we have chosen subgraphs S_i of $H_i - R$ so that $|E(S_i)| = p-1$ and $S_0+S_1+S_2+\cdots+S_{t-1}$ is acyclic. The number of components of $(H_t-R_k)+S_0+S_1+S_2+\cdots+S_{t-1} \ge c_{\overline{R}}(H_t) = p^{k-1}-(t+1)(p-1)$. Hence we may choose from $H_t-(R_k+S_0+S_1+S_2+\cdots+S_{t-1})$ a subgraph S_t of $p-1$ edges such that $S_0+S_1+S_2+\cdots+S_{t-1}+S_t$ is acyclic.

The acyclic subgraph $S_0+S_1+S_2+\cdots+S_{k-1}$ can be extended to a spanning tree T of $\textsc{Cay}(\mathbb{Z}_p^{k-1}; \{e_1, e_2, \ldots, e_{k-1}\}^\star)$. We finish the construction with the following two steps.

Step 1. If L_i is not a Hamilton cycle we use the $p-1$ edges of S_i to join its p cycles of length p^{k-1} into a Hamilton cycle and also to reduce the number of components in the 2-factor G as follows:

If C_1 and C_2 are two cycles in L_i then the edges $C_1 - R_k$ and $C_2 - R_k$ are parallel. Thus, because S_i is a maximal acyclic subgraph of $H_i - R_k$, there exists a pair of parallel edges $f_i = \{\vec{x}_i, \vec{y}_i\} \in E(C_i)$, $i = 1, 2$ such that the $\pi_{k-1}(\vec{f_1}) = \pi_{k-1}(\vec{f_2}) \in S_i$. We let F be the 4-cycle $\vec{x}_1\vec{y}_1\vec{y}_2\vec{x}_1$, and replace L_i with $L_i \triangle F$ and G with $G \triangle F$. This joins cycles C_1 and C_2 of L_i and joins the cycle in G containing the edge $\{\vec{x}_1, \vec{x}_2\}$ with the cycle containing the edge $\{\vec{y}_1, \vec{y}_2\}$.

Step 2. We now consider the edges of T that are not used in Step 1. For each pair of disjoint cycles C_1 and C_2 remaining in G. The projections $\pi_{k-1}(C_1)$ and $\pi_{k-1}(C_2)$ identify two components of $\textsc{Cay}(\mathbb{Z}_p^{k-1}; \{\vec{e}_1, \ldots, \vec{e}_{k-1}\}^\star)$ these two components are joined by a unique edge $f = \{\vec{x}, \vec{y}\}$ in T and this edges cannot have been used in Step 1. Thus the edges of X_k that project onto f all belong to the same subgraph L_i, which is now a Hamilton cycle by Step 1. There are p pairs of parallel edges that project onto f, consequently given an orientation of the cycle L_i there must exist a pair of parallel edges $\{\vec{x}_1, \vec{y}_1\}$ and $\{\vec{x}_2, \vec{y}_2\}$ such that $(\vec{x}_1, \vec{y}_1)$ and $(\vec{x}_2, \vec{y}_2)$ agree with the cycles orientation. We let F be the 4-cycle $\vec{x}_1\vec{y}_1\vec{y}_2\vec{x}_1$, and replace L_i with $L_i \triangle F$ and G with $G \triangle F$. This keeps L_i a Hamilton cycle and joins the the cycle in G containing the edge $\{\vec{x}_1, \vec{x}_2\}$ with the cycle containing the edge $\{\vec{y}_1, \vec{y}_2\}$.

Once all the edges of T have been processed in Step 1 or Step 2. The graph X_k has been decomposed into Hamilton cycles. It remains to be shown that this decomposition is special. But this is easy to see because no $\vec{r}$-edges were moved in Step 1 or Step 2. □

3.1 The finale

Now consider any subset $S \subseteq \mathbb{Z}_p^n$, such that $|S| = n+1$ and $X = \textsc{Cay}(\mathbb{Z}_p^n; S^\star)$ is connected then following the opening discussion to this section we may assume that $S = \{\vec{r}, \vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$. Without loss we may also assume that

$$\vec{r} = (r_1, r_2, \ldots, r_k, \underbrace{0, 0, \ldots, 0}_{n-k}),$$

where $r_i \neq 0$, for $i = 1, 2, \ldots, k$. Thus S may be partitioned into subsets $A = \{\vec{r}, \vec{e}_1, \vec{e}_2, \ldots, \vec{e}_k\}$ and $B = \{\vec{e}_{k+1}, \vec{e}_{k+2}, \ldots, \vec{e}_n\}$. These subsets are orthogonal and we may therefore apply Lemma 3.1 and consequently $X \approx X_1 \square X_2$, where $X_1 = \textsc{Cay}(\textsc{Span}(A); A^\star)$ and $X_2 = \textsc{Cay}(\textsc{Span}(B); B^\star) \approx \textsc{Cay}(\mathbb{Z}_p^{n-k}; \{e_1, e_2, \ldots, e_{n-k}\}^\star)$. If $k \ge 2$, then X_1 has a Hamilton decomposition by Theorem 1.5. If $k = 1$, then it has a Hamilton decomposition by Theorem 1.2. A Hamilton decomposition of X_2 follows from Corollary 3.3. Thus applying Stong's result, Theorem 1.1 a Hamilton decomposition of X is obtained thus proving Theorem 1.5.

In the next section we give an application of this Key Theorem.

4 Sub-Paley graphs

We are interested in a particular family of Cayley graphs on Abelian groups we call the Sub-Paley graphs.

Let $\mathbb{F}_q$ denote the finite field of order q. For even m dividing $q-1$ let $\mathrm{R}(q, m)$ be the unique multiplicative subgroup of $\mathbb{F}_q \setminus \{0\}$ of order m. We define the Sub-Paley graph $\mathrm{P}(q, m)$ of order q as the Cayley graph on $\mathbb{F}_q$ with connection set $\mathrm{R}(q, m)$. Hence, the vertices of $\mathrm{P}(q, m)$ are labeled with the elements of the field and there is an edge joining g and h if and only if $g - h \in \mathrm{R}(q, m)$. The reason we insist on h to be even is because then $\{1, -1\}$ is a subgroup of $\mathrm{R}(q, m)$ and

thus we have $g - h \in \mathrm{R}(q,m)$ if and only if $h - g \in \mathrm{R}(q,m)$. Because multiplicative subgroups of $\mathbb{F}_q \setminus \{0\}$ are cyclic, $\mathrm{R}(q,m) = \{1, \beta^1, \beta^2, \ldots, \beta^{m-1}\}$ for some $\beta \in \mathbb{F}_q$. Let $\mathrm{R}_h(q,m) = \{1, \beta^1, \beta^2, \ldots, \beta^{m/2-1}\}$. Then either $g \in \mathrm{R}_h(q,m)$ or $-g \in \mathrm{R}_h(q,m)$, but not both. Hence $|\mathrm{R}_h(q,m)| = m/2$ and $\mathrm{R}_h(q,m)^\star = \mathrm{R}(q,m)$.

Note that if $q \equiv 1 \pmod 4$, then $\mathrm{R}(q,(q-1)/2)$ is the set of quadratic residues and $\mathrm{P}(q,(q-1)/2)$ is the *Paley graph* of order q. In [2] all Paley graphs were shown to be Hamilton-decomposable.

Theorem 4.1 *Let $q = p^n$, where p an odd prime and let $m \geq 2n^2$ be an even divisor of $q-1$. If the sub-Paley graph $X = \mathrm{Cay}(\mathbb{F}_q; \mathrm{R}(q,m))$ is connected, then X is Hamilton-decomposable.*

Proof. Let $g(X)$ be the minimum polynomial for β over $\mathbb{F}_p$ and let $d = \deg(g(X))$. Then

$$A_0 = \{1, \beta, \beta^2, \ldots, \beta^{d-1}\}$$

considered as vectors over $\mathbb{F}_p$ is a maximal linear independent set in $\mathrm{R}_h(q,m)$. If the graph X is connected then $\mathrm{R}_h(q,m)$ must span $\mathbb{F}_q$ and therefore in this case $d = n$. Thus writing $m/2 = tn + r$, where $0 \leq r < n$ we partition $\mathrm{R}_h(q,m)$ into the linearly independent sets

$$A_0, A_1, \ldots, A_t$$

where

$$A_i = (\beta^d)^i A_0 = \{\beta^{di}, \beta^{di+1}, \ldots, \beta^{di+d-1}\},$$

$i = 0, 1, 2, \ldots, t-1$ and $A_t = \{\beta^{tn}, \beta^{tn+1}, \beta^{tn+2}, \ldots, \beta^{m/2-1}\}$. Now $t = \left\lfloor \frac{m}{2n} \right\rfloor \geq n > r$ Thus we may apply The Key Theorem to $A_j \cup \{\beta^{tn+j}\}$, for $j = 0, 1, 2, \ldots, m/2 - tn - 1$ decomposing $\mathrm{Cay}(\mathbb{F}_p; (A_j \cup \{\beta^{tn+j}\})$ into Hamilton cycles, for $j = 0, 1, 2, \ldots, m/2 - tn - 1$. We apply Theorem 3.3 to decompose $\mathrm{Cay}(\mathbb{F}_p; A_\ell)$ into Hamilton cycles for $\ell = m/2 - tn, m/2 - tn + 1, \ldots, t$. □

The result of Alspach, Bryant and Dyer on Paley graphs in [2] can be obtained as a simple consequence of Theorem 4.1.

Corollary 4.2 (Alspach, Bryant, Dyer, 2010) *All Paley graphs are Hamilton-decomposable.*

Proof. If $q = p^n \equiv 1 \pmod 4$, where p is a prime and n a positive integer, then it is elementary to show that $(q-1)/2 \geq 2n^2$, except when $q = 9$. Applying Theorem 4.1 we obtain the result. For $q = 9$ the Paley graph is 4 regular and is Hamilton decomposable by Theorem 1.2. □

Theorem 4.1 leaves open the sub-Paley graphs $X = \mathrm{Cay}(\mathbb{F}_q; \mathrm{R}(q,m))$, where q is odd and $2n \leq m < 2n^2$ or where q is even.

References

[1] B. Alspach, Research Problem 59, *Discrete Math.* **50** (1984), 115.

[2] B. Alspach, D. Bryant, D. Dyer, Paley Graphs Have Hamilton Decompositions, (2011) to appear.

[3] J.-C. Bermond, Hamilton decomposition of graphs directed graphs and hypergraphs, Advances in Graph Theory, *Annals of Discrete Math.* **3** (1978) 21-28.

[4] J.-C. Bermond, O. Favaron and M. Maheo, Hamiltonian decomposition of Cayley graphs of degree four, *J. Combin. Theory Ser. B* **46** (1989) 142-153.

[5] Jiuqiang Liu, Hamiltonian decomposition of Cayley graphs on Abelian groups, Discrete Mathematics **131** (1994) 163-171.

[6] R. Stong, Hamilton decompositions of Cartesian products of graphs, *Discrete Math.* **90** (1991) 169-190.

[7] E. Westlund, D. Kreher and J. Liu, 6-regular Cayley graphs on abelian groups of odd order are hamiltonian decomposable, *Discrete Math.* **309** (2009), 5106-5110.