New Series of Dudeney Sets for $p+2$ Vertices

Midori Kobayashi*
School of Administration and Informatics
University of Shizuoka
Shizuoka 422-8526
Japan

Nobuaki Mutoh
School of Administration and Informatics
University of Shizuoka
Shizuoka 422-8526
Japan

Kiyasu-Zen'iti
Semiconductor Research Institute
Sendaisi Aobaku Kawauti 980-0862
Japan

Gisaku Nakamura
Tokai University
Shibuyaku Tokyo 151-0063
Japan

Abstract

Dudeney's round table problem was proposed about one hundred years ago. It is already solved when the number of people is even, but it is still unsettled except only few cases when the number of people is odd.

In this paper, a solution of Dudeney's round table problem is given when $n = p + 2$, where p is an odd prime number such that 2 is the square of a primitive root of $GF(p)$, $p \equiv 1 \pmod 4$, and 3 is not a quadratic residue modulo p.

1 Introduction

A Dudeney set in K_n is a set of Hamilton cycles with the property that every path of length two (2-path) in K_n lies on exactly one of the cycles. We call the problem of construction a Dudeney set in K_n for all natural numbers "Dudeney's round table problem".

A Dudeney set in K_n has been constructed when n is even [3]. In the case n is odd, a Dudeney set in K_n has been constructed only when

*This research was supported in part by Grand-in-Aid for Scientific Research (C).

(1) $n = 2^k + 1$ (k is a natural number) [6],

(2) $n = p + 2$ (p is an odd prime number and 2 or -2 is a primitive root of $GF(p)$) [1,2],

(3) $n = p + 2$ (p is an odd prime number, 2 is the square of a primitive root of $GF(p)$ and $p \equiv 3 \pmod 4$) [2],

and some sporadic cases [1]. To construct a Dudeney set in K_n for a general odd integer $n > 0$, the case $n = p + 2$ (p is an odd prime number) has a central part. But in the case, it has been constructed only when (2) and (3). In this paper, we will show:

Theorem 1.1 *There exists a Dudeney set in K_n when $n = p + 2$, where p is an odd prime number such that 2 is the square of a primitive root of $GF(p)$, $p \equiv 1 \pmod 4$, and 3 is not a quadratic residue modulo p.*

The method of constructing a Dudeney set given here is new. In paper [2], the method of exchanging edges was used so the proof of hamiltonicity was important. In this paper, however, hamiltonicity is trivial because we use the transformation ξ. This is the main advantage of our method.

We should mention the case when -2 is the square of a primitive root of $GF(p)$. In this case, we have a similar theorem.

Theorem 1.2 *There exists a Dudeney set in K_n when $n = p + 2$, where p is an odd prime number such that -2 is the square of a primitive root of $GF(p)$, and either*
(1) $p \equiv 1 \pmod 4$, *and 3 is not a quadratic residue modulo p, or*
(2) $p \equiv 3 \pmod 4$.

Theorem 1.2 is trivial from Lemma 1.3, Theorem 1.1 and the known results.

Lemma 1.3 *Let p be an odd prime number.*
(1) *When $p \equiv 1 \pmod 4$, -2 is the square of a primitive root of $GF(p)$ if and only if 2 is the square of a primitive root of $GF(p)$.*
(2) *When $p \equiv 3 \pmod 4$, -2 is the square of a primitive root of $GF(p)$ if and only if 2 is a primitive root of $GF(p)$.*

Proof. Put $r = (p-1)/2$.
(1) When $p \equiv 1 \pmod 4$, r is even. If -2 is the square of a primitive root, 2 is a quadratic residue, so we have $p \equiv 1 \pmod 8$. If $-2 = \omega^2$, where ω is a primitive root, then $2 = \omega^{r+2} = (\omega^{(r+2)/2})^2$. Since $((r+2)/2, p-1) = 1$, 2 is the square of a primitive root, where $(\ ,\ )$ means the greatest common divisor. The converse is similar.

(2) When $p \equiv 3 \pmod 4$, r is odd.

If $-2 = \omega^2$, where ω is a primitive root, then $2 = \omega^{r+2}$. Since $(r+2, p-1) = 1$, 2 is a primitive root. Conversely, if 2 is a primitive root, then $-2 = (2^{(r+1)/2})^2$. Since 2 is not a quadratic residue, we have $p \equiv 3 \pmod 8$. So we have $((r+1)/2, p-1) = 1$ and $2^{(r+1)/2}$ is a primitive root. □

2 Preliminaries

Put $n_1 = p+1$, where p is an odd prime number, and $r = (p-1)/2$. We denote by $K_{n_1} = (V_{n_1}, E_{n_1})$ the complete graph on n_1 vertices, where $V_{n_1} = \{0, 1, 2, \cdots, p-1\} \cup \{\infty\} = Z_p \cup \{\infty\}$ is the vertex set (Z_p is the set of integers modulo p).

For any integer i, $0 \le i \le p-1$, define the 1-factors

$$F_i = \{\{\infty, i\}\} \cup \{\{a, b\} \in E_{n_1} \mid a, b \neq \infty, a + b \equiv 2i \pmod p\}$$
$$I_i = \{\{\infty, i/2\}\} \cup \{\{a, b\} \in E_{n_1} \mid a, b \neq \infty, a + b \equiv i \pmod p\}.$$

Note that $F_i = 2I_i$, where multiplication is considered modulo p and we define $a \times \infty = \infty$ ($a \neq 0$).

Let σ be the vertex-permutation $(\infty)(0\ 1\ 2\ \ldots\ p-1)$, and put $\Sigma = \{\sigma^j \mid 0 \le j \le p-1\}$. When $\mathcal{C}$ is a set of cycles or circuits in K_{n_1}, define $\Sigma\mathcal{C} = \{C^\tau \mid C \in \mathcal{C}, \tau \in \Sigma\}$.

For any edge $\{a, b\}$ in K_{n_1}, we define the length $d(a, b)$:

$$d(a,b) = \begin{cases} b - a \pmod p & (a, b \neq \infty) \\ \infty & (\text{otherwise}), \end{cases}$$

where we define that lengths c_1, c_2 are equal if $c_1 = c_2$ or $c_1 = -c_2 \pmod p$.

A set $H \subset Z_p^* = Z_p \setminus \{0\}$ is called a half-set modulo p if $|H| = (p-1)/2$ and $H \cup (-H) = Z_p^*$.

A sequence of non-zero intergers $d = (d_1, d_2, \cdots, d_t)$ is called a difference sequence of length t. Each component d_i is considered modulo p. We usually write d_i satisfying $-r \le d_i \le r$. For two difference sequences $d = (d_1, d_2, \cdots, d_t)$ and $d' = (d'_1, d'_2, \cdots, d'_t)$, we define $d = d'$ when $d_1 = d'_1, d_2 = d'_2, \cdots, d_t = d'_t$ or $d_1 = -d'_t, d_2 = -d'_{t-1}, \cdots, d_t = -d'_1$.

For an l-path $P = (a_0, a_1, \cdots, a_l)$ ($a_i \neq \infty (0 \le i \le l)$) in K_{n_1}, we define the difference sequence of P:

$$d(P) = (a_1 - a_0, a_2 - a_1, \cdots, a_l - a_{l-1}).$$

Lemma 2.1 *Let P_1, P_2 be l-paths in K_{n_1} not containing ∞. Then $d(P_1) = d(P_2)$ if and only if $P_2 = P_1^{\sigma^i}$ for some i, $0 \le i \le p-1$.*

We define the difference sequence of an Hamilton cycle in K_{n_1} as follows. Write a Hamilton cycle with ∞ the first. For a Hamilton cycle

$$C = (\infty, a_1, a_2, \cdots, a_p),$$

define the difference sequence of C:

$$d(C) = (a_2 - a_1, a_3 - a_2, \cdots, a_p - a_{p-1}).$$

Lemma 2.2 *Let C_1, C_2 be Hamilton cycles in K_{n_1}. Then $d(C_1) = d(C_2)$ if and only if $C_2 = C_1^{\sigma^i}$ for some i, $0 \leq i \leq p-1$.*

For a difference sequence $d = (a_1, a_2, \cdots, a_{p-1})$ of length $p-1$, we call $W(d) = (\infty, 0, a_1, a_1 + a_2, \cdots, \sum_{i=1}^{p-1} a_i)$ the representative Hamilton cycle of d, if $W(d)$ is a Hamilton cycle in K_{n_1}.

A difference sequence $d = (d_1, d_2, \cdots, d_{p-1})$ of length $p-1$ is symmetric if $d_i = d_{p-i}$ $(1 \leq i \leq r)$.

We next construct the complete graph K_n by adding a new vertex λ to K_{n_1}; that is, put $n = n_1 + 1 = p + 2$, $K_n = (V_n, E_n)$ and $V_n = V_{n_1} \cup \{\lambda\}$. Extend σ to a permutation of V_n and denote it also by σ: $\sigma = (\infty)(\lambda)(0\ 1\ 2\ 3\ \cdots\ p-1)$. Further we put $\Sigma = \{\sigma^j \mid 0 \leq j \leq p-1\}$.

Let A be a 1-factor in K_{n_1} which satisfies 1 and 2:

1. *$F_0 \cup A$ is a Hamilton cycle in K_{n_1}.*
2. *If S is the multiset $\{d(a,b) \mid \{a,b\} \in A\}$, then we have $S = \{\infty, 1, 2, \cdots, r\}$, i.e. A has all lengths.*

If we insert the vertex λ into all the edges in A, we get a set of 2-paths in K_n. Denote this set by A^λ; that is,

$$A^\lambda = \{(a, \lambda, b) \mid \{a,b\} \in A\}.$$

We note that paths are undirected, i.e., $(a, \lambda, b) = (b, \lambda, a)$. $F_0 \cup A^\lambda$ is considered to be a circuit in K_n.

Proposition 2.3 *Assume h_i $(1 \leq i \leq r)$ is a Hamilton cycle in K_{n_1} and $\Sigma\{h_i \mid 1 \leq i \leq r\}$ is a Dudeney set in K_{n_1}. Then*

$$\Sigma(\{F_0 \cup A^\lambda\} \cup \{h_i \mid 1 \leq i \leq r\})$$

has every 2-path in K_n exactly once.

Proof. Divide the set of all 2-paths in K_n into 8 classes:
(i) (a,b,c), (ii) (a,∞,b), (iii) (∞,a,b), (iv) (a,λ,b), (v) (λ,a,b), (vi) (λ,∞,a), (vii) (λ,a,∞), (viii) (∞,λ,a), where $a,b,c \neq \infty,\lambda$.

(i), (ii), (iii) are also 2-paths in K_{n_1}, so they belong to $\Sigma\{h_i \mid 1 \leq i \leq r\}$.

(iv), (viii) Since A has all lengths, we have $\Sigma A = E_{n_1}$. Hence 2-paths (a, λ, b) and (∞, λ, a) belong to ΣA^λ. So (a, λ, b) and (∞, λ, a) belong to $\Sigma\{F_0 \cup A^\lambda\}$.

(v) We have $\{a, b\}^{\sigma^t} \in F_0$ for some t $(0 \leq t \leq p-1)$, as F_0 has all lengths. So we can assume $\{a, b\} \in F_0$ without loss of generality. Since A is a 1-factor, we have $\{a, c\} \in A$ for some $c \in V_{n_1}$. Then we have $(a, \lambda, c) \in A^\lambda$. So (λ, a, b) belongs to $F_0 \cup A^\lambda$

(vi), (vii) Similarly, we can assume $a = 0$. The 2-paths $(\lambda, \infty, 0)$ and $(\lambda, 0, \infty)$ belong to $F_0 \cup A^\lambda$.

By counting the number of 2-paths, we prove that every 2-path in K_n lies only once. □

3 Definition of $h(0)$

From now to the end of this paper, we assume that p is an odd prime number with $p \equiv 1 \pmod 4$, $p \geq 41$, and that 2 is the square of a primitive root of $GF(p)$ and 3 is not a quadratic residue modulo p.

Put $n_1 = p + 1$, $r = (p-1)/2$ same as before and put $s = r/2$.

Lemma 3.1 *Under our assumption of p, s is even.*

Proof. Since $(\frac{2}{p}) = 1$, we have $p \equiv 1$ or $7 \pmod 8$, and since $(\frac{3}{p}) = (\frac{p}{3}) = -1$, we have $p \equiv 2 \pmod 3$, where $(\ )$ is the Legendre symbol. Together with $p \equiv 1 \pmod 4$, we obtain $p \equiv 17 \pmod{24}$ which follows that s is even. □

Define four paths A, B, C, D;

$$A = (1, -1, -2, 2, 2^2, -2^2, -2^3, 2^3, \cdots, -2^{s-1}, 2^{s-1}, 0)$$
$$B = (3^{-1}2, -3^{-1}2, -3^{-1}2^2, 3^{-1}2^2, 3^{-1}2^3, -3^{-1}2^3, \cdots, -3^{-1}2^s, 3^{-1}2^s, \infty)$$
$$C = (1, 3^{-1}2)$$
$$D = (0, \infty)$$

and define the Hamilton cycle in K_{n_1},

$$h(0) = A \cup B \cup C \cup D,$$

where $\cup$ means concatenation of paths. Note that $2^{s-1} = r$, $3^{-1}2^s = -3^{-1}$.

As $h(0)$ contains the 1-factor F_0, we can write $h(0) = F_0 \cup G$ where G is a 1-factor in K_{n_1}.

Lemma 3.2 *If S is the multiset $\{d(a, b) \mid \{a, b\} \in G\}$, then we have $S = \{\infty, 1, 2, \cdots, r\}$, i.e. G has all lengths.*

Proof. From our assumption, it holds $GF(p)^* = \langle 2 \rangle \cup 3\langle 2 \rangle$, where $\langle 2 \rangle = \{1, 2, 2^2, \cdots, 2^{s-1}, -1, -2, -2^2, \cdots, -2^{s-1}\}$. Define

$$\begin{aligned} G_A &= \{\{-1,-2\},\{2,2^2\},\{-2^2,-2^3\},\cdots,\{-2^{s-2},-2^{s-1}\}\} \\ G_B &= \{\{-3^{-1}2,-3^{-1}2^2\},\{3^{-1}2^2,3^{-1}2^3\},\{-3^{-1}2^3,-3^{-1}2^4\},\cdots, \\ &\quad \{-3^{-1}2^{s-1},-3^{-1}2^s\}\} \\ G_C &= \{\{1,3^{-1}2\}\} \\ G_D &= \{\{2^{s-1},0\},\{3^{-1}2^s,\infty\}\} \end{aligned}$$

then we have $G = G_A \cup G_B \cup G_C \cup G_D$.

$$\begin{aligned} &G_A \text{ has lengths } 1, 2, 2^2, \cdots, 2^{s-2} \\ &G_B \text{ has lengths } 3^{-1}2, 3^{-1}2^2, \cdots, 3^{-1}2^{s-1} \\ &G_C \text{ has lengths } 3^{-1} \\ &G_D \text{ has lengths } 2^{s-1}, \infty. \end{aligned}$$

Hence G has all lengths. □

4 Conditions of $h(1)$

We would like to construct a Hamilton cycle $h(1)$ in K_{n_1} satisfying the following 3 conditions:

1. $\Sigma\{ah(1) \mid a \in H\}$ is a Dudeney set in K_{n_1} for any half-set H modulo p.
2. $h(1)$ has the 5-path $(\infty, 0, 1, -1, -2, 2)$.
3. $h(1)$ has the 3-path $(-2, 2, 3, -3)$.

We will construct $h(1)$ from the Hamilton cycle

$$F_0 \cup I_1 = (\infty,\ 0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3, \cdots, r,\ -r).$$

The difference sequence d of $F_0 \cup I_1$ is

$$d = (1, -2, 3, -4, \cdots, -r; -r, \cdots, -4, 3, -2, 1),$$

and d is symmetric.

For a symmetric difference sequence

$$d = (d_1, d_2, \cdots, d_{2r})$$

of length $2r$, we define Property (A):

Property (A): For any half-set H modulo p, $\{id \mid i \in H\}$ has the difference sequences of all 2-paths (a,b,c) in K_{n_1} with $a,b,c \neq \infty$ exactly once, i.e.,

$$\{i(d_j, d_{j+1}) \mid 1 \leq j \leq 2r-1, i \in H\}$$
$$= \{(b-a, c-b) \mid (a,b,c) \text{ is a } 2-\text{path in } K_{n_1} \text{with } a,b,c \neq \infty\},$$

where equality is one as sets of difference sequences.

Lemma 4.1 *Let W be a Hamilton cycle in K_{n_1}. Let H be a half-set modulo p. Then*

$$\Sigma\{iW \mid i \in H\} = \cup_{i \in H} i(\Sigma W).$$

Proof.

$$\begin{aligned} L &= \Sigma\{iW \mid i \in H\} \\ &= \{iW + j \mid i \in H, 0 \leq j \leq p-1\}, \text{ and} \\ R &= \cup_{i \in H} i(\Sigma W) \\ &= \{i(W+j) \mid i \in H, 0 \leq j \leq p-1\} \\ &= \{iW + ij \mid i \in H, 0 \leq j \leq p-1\}, \end{aligned}$$

so we have $L = R$. □

Proposition 4.2 *Let $d = (d_1, d_2, \cdots, d_{2r})$ be a symmetric difference sequence of length $2r$. Assume that $W = W(d)$ is the representative Hamilton cycle of d in K_{n_1}. Then (1) and (2) are equivalent.*

(1) *d has Property* (A).

(2) *$\Sigma\{iW \mid i \in H\}$ has all 2-paths in K_{n_1} for any half-set H modulo p.*

Proof. (2) → (1)

Let H be a half-set modulo p. Let (a,b,c) be any 2-path in K_{n_1} with $a,b,c \neq \infty$. The 2-path (a,b,c) belongs to $\Sigma\{iW \mid i \in H\}$, so the difference sequence $(b-a, c-b)$ belongs to $\{id \mid i \in H\}$. Note that $W(id) = iW(d)$.

(1) → (2)

Let H be a half-set modulo p and put $\mathcal{W} = \Sigma\{iW \mid i \in H\}$. Let $P = (a,b,c)$ be any 2-path in K_{n_1}.

(i) When $a,b,c \neq \infty$, $(b-a, c-b)$ belongs to id for some $i \in H$, so $P = (a,b,c)$ belongs to $\Sigma\{iW\}$ so belongs to $\mathcal{W}$.

(ii) When $a = \infty$, we have $P = (\infty, b, c)$. We will show that P belongs to $\mathcal{W}$. We may assume $b = 0$ without loss of generality. (If necessary, apply σ^{-b} to P, then we obtain $(\infty, 0, c-b)$.)

Now $P = (\infty, 0, c)$ with $c \neq \infty, 0$. Since d is symmetric, we have $d_{2r} = d_1$, so W has 2-paths $(\infty, 0, d_1)$ and $(x, x+d_1, \infty)$, where $x = \sum_{i=1}^{2r-1} d_i$.

Since $(x, x+d_1, \infty)^{\sigma^{-x-d_1}} = (-d_1, 0, \infty)$, ΣW has 2-paths $(\infty, 0, d_1)$ and $(-d_1, 0, \infty)$.

If $c = id_1$ for some $i \in H$, we have $(\infty, 0, c) = i(\infty, 0, d_1)$, then 2-path $(\infty, 0, c)$ belongs to $i(\Sigma W)$. Otherwise, $c = -id_1$ for some $i \in H$ as $d_1 \neq 0$ and H is a half-set. Then the 2-path $(\infty, 0, c)$ belongs to $i(\Sigma W)$ since $(\infty, 0, c) = i(\infty, 0, -d_1)$. In both cases $(\infty, 0, c)$ belongs to $\cup_{i \in H} i(\Sigma W)$, which is $\mathcal{W}$ by Lemma 4.1.

(iii) When $b = \infty$, we have $P = (a, \infty, c)$. We will show that P belongs to $\mathcal{W}$. We may assume $a = 0$ without loss of generality. Now $P = (0, \infty, c)$. W has 2-paths $(0, \infty, x)$, where $x = \sum_{j=1}^{2r} d_j$. Note that $x \neq 0$ because W is a Hamilton cycle.

If $c = ix$ for some $i \in H$, the 2-path $P = (0, \infty, c)$ belongs to iW. Otherwise, $c = -ix$ for some $i \in H$. Then the 2-path $P = (0, \infty, c)$ belongs to $\Sigma(iW)$ since $(0, \infty, c) = (i(x, \infty, 0))^{\sigma^c}$. In both cases, P belongs to $\mathcal{W}$. □

Proposition 4.3 *The difference sequence of $F_0 \cup I_1$ has Property* (A).

Proof. It is well-known that $\Sigma\{i(F_0 \cup I_1) \mid i \in H\}$ is a Dudeney set for any half-set H modulo p. So the difference sequence of $F_0 \cup I_1$ has Property (A) by Prop. 4.2. □

5 Transformation of difference sequences: $\xi(a)$

Let $d = (d_1, d_2, \cdots, d_r; d_r, \cdots, d_2, d_1)$ be a symmetric difference sequence with $-r \leq d_i \leq r$, $d_i \neq 0$ $(1 \leq i \leq r)$.

Let a be an integer with $-r \leq a \leq r, a \neq 0, \pm 1, \pm r$. We define the transformation $\xi(a)$ of difference sequences as follows.

(i) The case $a > 0$.

If $(-(a-1), a, -(a+1))$ appears in the first half of d in this order, we define the transformation $\xi(a)$ from d to $\xi(a)d$ as follows.

If

$$d = (d_1, d_2, \cdots, d_{t_1}, -(a-1), a, -(a+1), d_{t_1+4}, \cdots, d_r;$$
$$d_r, \cdots, d_{t_1+4}, -(a+1), a, -(a-1), d_{t_1}, \cdots, d_2, d_1),$$

then

$$\xi(a)d = (d_1, d_2, \cdots, d_{t_1}, -(a-1), -1, (a+1), -d_{t_1+4}, \cdots, -d_r;$$
$$-d_r, \cdots, -d_{t_1+4}, (a+1), -1, -(a-1), d_{t_1}, \cdots, d_2, d_1),$$

that is to say, $\xi(a)$ changes a to -1, changes the sign from $-(a+1)$ to d_r, and then makes $\xi(a)d$ symmetric.

(ii) The case $a < 0$.

If $(-(a+1), a, -(a-1))$ appears in the first half of d in this order, that is,

$$d = (d_1, d_2, \cdots, d_{t_1}, -(a+1), a, -(a-1), d_{t_1+4}, \cdots, d_r;$$
$$d_r, \cdots, d_{t_1+4}, -(a-1), a, -(a+1), d_{t_1}, \cdots, d_2, d_1),$$

then

$$\xi(a)d = (d_1, d_2, \cdots, d_{t_1}, -(a+1), 1, (a-1), -d_{t_1+4}, \cdots, -d_r;$$
$$-d_r, \cdots, -d_{t_1+4}, (a-1), 1, -(a+1), d_{t_1}, \cdots, d_2, d_1).$$

When d has Property (A), $\xi(a)d$ doesn't generally have Property (A). To make $\xi(a)d$ to have Property (A) we should transform $\xi(a)d$ by $\xi(b)$ for some b. Prop. 5.1 gives the number b.

Proposition 5.1 *Let $d = (d_1, d_2, \cdots, d_r; d_r, \cdots, d_2, d_1)$ be a symmetric difference sequence, where $-r \leq d_i \leq r, d_i \neq 0$ $(1 \leq i \leq r)$. Assume d has Property* (A). *Let $d_1 = \xi(a)d$, where $-r \leq a \leq r$, $a \neq 0, \pm 1, \pm r$. Let b be an integer with $-r \leq b \leq r$ satisfying $b \equiv a^{-1}$ or $b \equiv -a^{-1}$* (mod p), *then we have $b \neq 0, \pm 1$.*

(1) *The case $b > 0$. If $(-(b-1), b, -(b+1))$ appears in the first half of d_1 in this order, put $d_2 = \xi(b)d_1$. Then d_2 is a symmetric difference sequence and has Property* (A).

(2) *The case $b < 0$. If $(-(b+1), b, -(b-1))$ appears in the first half of d_1 in this order, put $d_2 = \xi(b)d_1$. Then d_2 is a symmetric difference sequence and has Property* (A).

Proof. (1) (a) Assume $a > 0$. d_1 has $(-(a-1), -1, (a+1))$ in the first half. We consider only when $(-(b-1), b, -(b+1))$ is on the right side of $(-(a-1), -1, (a+1))$ in d_1, including the case that $a+1 = -(b-1)$. When $(-(b-1), b, -(b+1))$ is on the left side, the proof is similar.

Then we have

$$d = (d_1, \cdots, d_{t_1}, -(a-1), a, -(a+1), d_{t_1+4}, \cdots, d_{t_2}, (b-1), -b, (b+1),$$
$$d_{t_2+4}, \cdots, d_r; d_r, \cdots, d_{t_2+4}, (b+1), -b, (b-1), d_{t_2}, \cdots, d_{t_1+4},$$
$$-(a+1), a, -(a-1), d_{t_1}, \cdots, d_1),$$
$$d_1 = (d_1, \cdots, d_{t_1}, -(a-1), -1, (a+1), -d_{t_1+4}, \cdots, -d_{t_2}, -(b-1), b,$$
$$-(b+1), -d_{t_2+4}, \cdots, -d_r; -d_r, \cdots, -d_{t_2+4}, -(b+1), b, -(b-1),$$
$$-d_{t_2}, \cdots, -d_{t_1+4}, (a+1), -1, -(a-1), d_{t_1}, \cdots, d_1),$$
$$d_2 = (d_1, \cdots, d_{t_1}, -(a-1), -1, (a+1), -d_{t_1+4}, \cdots, -d_{t_2}, -(b-1), -1,$$
$$(b+1), d_{t_2+4}, \cdots, d_r; d_r, \cdots, d_{t_2+4}, (b+1), -1, -(b-1), -d_{t_2}, \cdots,$$
$$-d_{t_1+4}, (a+1), -1, -(a-1), d_{t_1}, \cdots, d_1).$$

We consider the following 9 subsequences of d and d_2. The subsequences of d are on the left sides and the subsequences of d_2 are on the right sides of arrows. If $a+1=-(b-1)$, (iii) and (vii) are omitted.

(i) $(d_1,\cdots,d_{t_1},-(a-1)) \longrightarrow (d_1,\cdots,d_{t_1},-(a-1))$

(ii) $(-(a-1),a,-(a+1)) \longrightarrow (-(a-1),-1,(a+1))$

(iii) $(-(a+1),d_{t_1+4},\cdots,d_{t_2},(b-1))$
$\longrightarrow ((a+1),-d_{t_1+4},\cdots,-d_{t_2},-(b-1))$

(iv) $((b-1),-b,(b+1)) \longrightarrow (-(b-1),-1,(b+1))$

(v) $((b+1),d_{t_2+4},\cdots,d_r;d_r,\cdots,d_{t_2+4},(b+1))$
$\longrightarrow ((b+1),d_{t_2+4},\cdots,d_r;d_r,\cdots,d_{t_2+4},(b+1))$

(vi) $((b+1),-b,(b-1)) \longrightarrow ((b+1),-1,-(b-1))$

(vii) $((b-1),d_{t_2},\cdots,d_{t_1+4},-(a+1))$
$\longrightarrow (-(b-1),-d_{t_2},\cdots,-d_{t_1+4},(a+1))$

(viii) $(-(a+1),a,-(a-1)) \longrightarrow ((a+1),-1,-(a-1))$

(ix) $(-(a-1),d_{t_1},\cdots,d_1) \longrightarrow (-(a-1),d_{t_1},\cdots,d_1)$

The left sides and the right sides of (i), (v), (ix) are the same sequences, respectively. The left side of (iii) is the same as the right side of (vii) and the left side of (vii) is the same as the right side of (iii) as difference sequences.

Let H be a half-set modulo p. We will show that

$$\{i(-(a-1),a,-(a+1))\mid i\in H\}\cup\{i(-(a+1),a,-(a-1))\mid i\in H\}$$
$$=\{i(-(b-1),-1,(b+1))\mid i\in H\}\cup\{i((b+1),-1,-(b-1))\mid i\in H\},$$

as sets of difference sequences. To show it, we may show

$$\{i(-(a-1),a,-(a+1))\mid i\in Z_p^*\}=\{i(-(b-1),-1,(b+1))\mid i\in Z_p^*\} \quad (5.1)$$

because

$$\begin{aligned}(-1)(-(a-1),a,-(a+1)) &= ((a-1),-a,(a+1))\\ &= (-(a+1),a,-(a-1)),\\ (-1)(-(b-1),-1,(b+1)) &= ((b-1),1,-(b+1))\\ &= ((b+1),-1,-(b-1)),\end{aligned}$$

and $H\cup(-1)H=Z_p^*$. If $b\equiv a^{-1}$, then

$$-a^{-1}(-(a-1),a,-(a+1))=(-(b-1),-1,(b+1)),$$

and if $b \equiv -a^{-1}$, then

$$a^{-1}(-(a-1), a, -(a+1)) = (-(b+1), 1, (b-1)) = (-(b-1), -1, (b+1)).$$

So (5.1) holds. Therefore the left sides of (ii) and (viii) are the same as the right sides of (iv) and (vi), by multiplying by elements of H.

Next we will show that

$$\{i(-(a-1), -1, (a+1)) \mid i \in H\} \cup \{i((a+1), -1, -(a-1)) \mid i \in H\}$$
$$= \{i((b-1), -b, (b+1)) \mid i \in H\} \cup \{i((b+1), -b, (b-1)) \mid i \in H\}.$$

To show it, we may show

$$\{i(-(a-1), -1, (a+1)) \mid i \in Z_p^*\} = \{i((b-1), -b, (b+1)) \mid i \in Z_p^*\}. \quad (5.2)$$

Since

$$a^{-1}(-(a-1), -1, (a+1)) = ((b-1), -b, (b+1)),$$

(5.2) holds. Therefore the left sides of (iv) and (vi) are the same as the right sides of (ii) and (viii), by multiplying by elements of H.

Hence we have

$$\{id \mid i \in H\} = \{id_2 \mid i \in H\},$$

so d_2 has Property (A) since d has Property (A).

(b) Assume $a < 0$. d_1 has $(-(a+1), 1, (a-1))$ in the first half. We consider only when $(-(b-1), b, -(b+1))$ is on the right side of $(-(a+1), 1, (a-1))$ in d_1. Then we have

$$\begin{aligned}
d = (&d_1, \cdots, d_{t_1}, -(a+1), a, -(a-1), d_{t_1+4}, \cdots, d_{t_2}, (b-1), -b, (b+1),\\
&d_{t_2+4}, \cdots, d_r; d_r, \cdots, d_{t_2+4}, (b+1), -b, (b-1), d_{t_2}, \cdots, d_{t_1+4},\\
&-(a-1), a, -(a+1), d_{t_1}, \cdots, d_1),\\
d_1 = (&d_1, \cdots, d_{t_1}, -(a+1), 1, (a-1), -d_{t_1+4}, \cdots, -d_{t_2}, -(b-1), b,\\
&-(b+1), -d_{t_2+4}, \cdots, -d_r; -d_r, \cdots, -d_{t_2+4}, -(b+1), b, -(b-1),\\
&-d_{t_2}, \cdots, -d_{t_1+4}, (a-1), 1, -(a+1), d_{t_1}, \cdots, d_1),\\
d_2 = (&d_1, \cdots, d_{t_1}, -(a+1), 1, (a-1), -d_{t_1+4}, \cdots, -d_{t_2}, -(b-1), -1,\\
&(b+1), d_{t_2+4}, \cdots, d_r; d_r, \cdots, d_{t_2+4}, (b+1), -1, -(b-1), -d_{t_2}, \cdots,\\
&-d_{t_1+4}, (a-1), 1, -(a+1), d_{t_1}, \cdots, d_1).
\end{aligned}$$

Similarly, we have $\{id \mid i \in H\} = \{id_2 \mid i \in H\}$ for any half-set H, so d_2 has Property (A).

(2) The proof is similar to that of (1). □

6 Construction of $h(1)$

We construct the Hamilton cycle $h(1)$ satisfying conditions 1, 2 and 3 in this section. Let d be the difference sequence of $F_0 \cup I_1$. Then we have $W(d) = F_0 \cup I_1$. $W(d)$ satisfies condition 1, i.e., $\Sigma\{iW(d) \mid i \in H\}$ is a Dudeney set, but does not satisfy conditions 2 and 3. The difference sequence d has Property (A) by Prop. 4.3 and d has $(-2, 3, -4)$ in the first half. Put $d_1 = \xi(3)d$, then we have

$$d_1 = (1, -2, -1, 4, -5, 6, -7, \cdots, -(r-1), r;$$
$$r, -(r-1), \cdots, -7, 6, -5, 4, -1, -2, 1).$$

Note that $W(d_1) = (\infty, 0, 1, -1, -2, 2, -3, 3, -4, 4, \cdots)$, so it satisfies condition 2. Put $p = 24k+17$ (k is a natural number), then we have $3^{-1} = 8k+6$ which is even and $14 \leq 8k + 6 \leq r - 2$. Therefore Lemma 6.1 holds.

Lemma 6.1 *The difference sequence d_1 has $(-(3^{-1}-1), 3^{-1}, -(3^{-1}+1))$ in the first half.*

Put $d_2 = \xi(3^{-1})d_1$, then we have

$$d_1 = (1, -2, -1, 4, -5, 6, -7, \cdots, -(8k+5), (8k+6), -(8k+7), \cdots,$$
$$-(r-1), r; \cdots)$$
$$d_2 = (1, -2, -1, 4, -5, 6, -7, \cdots, -(8k+5), -1, (8k+7), \cdots, (r-1), -r;$$
$$\cdots)$$

Proposition 6.2 *$W(d_2)$ is a Hamilton cycle and it satisfies conditions* 1 *and* 2.

Proof. It is trivial that $W(d_2)$ is a Hamilton cycle (see Figure 1). d_2 has Property (A) by Prop. 5.1, hence $W(d_2)$ satisfies condition 1 by Prop. 4.2 and that $W(d_2)$ is a Hamilton cycle. We have $W(d_2) = (\infty, 0, 1, -1, -2, 2, \cdots)$, so it satisfies condition 2. □

Next we consider about condition 3. The difference sequence of the 3-path $(-2, 2, 3, -3)$ is $(4, 1, -6)$. d_2 still has the difference sequence $(4, -5, 6)$ in the first half because $3^{-1} = 8k + 6 \geq 14$. Put $d_3 = \xi(-5)d_2$, then we have

$$d_3 = (1, -2, -1, 4, 1, -6, 7, \cdots).$$

Let b be an integer with $1 \leq b \leq r$ satisfying $b \equiv 5^{-1}$ or $b \equiv -5^{-1} \pmod{p}$. d has trivially $(-(b-1), b, -(b+1))$ or $((b-1), -b, (b+1))$ in the first half. So d_3 still has $(-(b-1), b, -(b+1))$ or $((b-1), -b, (b+1))$ in the first half, since $8 \leq b \leq r - 1$ and $b \neq 8k + 5, 8k + 6, 8k + 7$. Therefore Lemma 6.3 holds.

Lemma 6.3 $(-(b-1), b, -(b+1))$ *or* $((b-1), -b, (b+1))$ *appears in the first half of* d_3.

If $(-(b-1), b, -(b+1))$ appears in the first half of d_3, put $d_4 = \xi(b)d_3$. If $((b-1), -b, (b+1))$ appears in the first half of d_3, put $d_4 = \xi(-b)d_3$.

Proposition 6.4 $W(d_4)$ *is a Hamilton cycle and it satisfies conditions* 1, 2 *and* 3.

Proof. It is trivial that $W(d_4)$ is a Hamilton cycle (see Figure 2). d_4 has property (A) by Prop. 5.1, hence it satisfies condition 1 by Prop. 4.2 and that $W(d_4)$ is a Hamilton cycle. Since

$$d_4 = (1, -2, -1, 4, 1, -6, 7, \cdots),$$

we have

$$W(d_4) = (\infty, 0, 1, -1, -2, 2, 3, -3, 4, \cdots),$$

which contains the 5-path $(\infty, 0, 1, -1, -2, 2)$ and the 3-path $(-2, 2, 3, -3)$, so it satisfies conditions 2 and 3. □

Therefore we put $h(1) = W(d_4)$ from now on.

7 Construction of a Dudeney set

Let G be the 1-factor with $h(0) = F_0 \cup G$. Insert the vertex λ into all edges in G and define G^λ same as before; that is,

$$G^\lambda = \{(a, \lambda, b) \mid \{a, b\} \in G\}.$$

Put $h(a) = ah(1)$, where a is an integer $\neq 0$. Since G has all lengths (Lemma 3.2), we obtain by Prop. 2.3,

Proposition 7.1 *Let* H *be a half-set modulo* p. *Then*

$$\Sigma(\{F_0 \cup G^\lambda\} \cup \{h(a) \mid a \in H\})$$

has every 2-path in K_n *exactly once.*

We would like to leave one λ in $F_0 \cup G^\lambda$ and scatter the remaining r λs over $\{h(a) \mid a \in H\}$. Remember $G = G_A \cup G_B \cup G_C \cup G_D$. We consider λs in these 4 subsets of G each.

(1) G_A

It holds that $G_A = \{(-2)^i\{-1, -2\} \mid 0 \leq i \leq s-2\}$. Put $H_1 = \{(-2)^i \mid 0 \leq i \leq s-2\}$. As $h(1)$ has a 3-path $(1, -1, -2, 2)$, $h((-2)^i)$ has a 3-path $((-2)^i, -(-2)^i, -2(-2)^i, 2(-2)^i)$. Denote $h((-2)^i)^\lambda$ the cycle in

K_n obtained from $h((-2)^i)$ inserting λ into the center of this 3-path, i.e., inserting λ between $-(-2)^i$ and $-2(-2)^i$.

(2) G_B

It holds that $G_B = \{3^{-1}2(-2)^i\{-1,-2\} \mid 0 \leq i \leq s-2\}$. Put $H_2 = \{3^{-1}2(-2)^i \mid 0 \leq i \leq s-2\}$. $h(3^{-1}2(-2)^i)$ has a 3-path $(3^{-1}2(-2)^i, -3^{-1}2(-2)^i, -3^{-1}4(-2)^i, 3^{-1}4(-2)^i)$. Denote $h(3^{-1}2(-2)^i)^\lambda$ the cycle obtained from $h(3^{-1}2(-2)^i)$ inserting λ into the center of this 3-path.

(3) G_C

As $h(1)$ has the 3-path $(-3,3,2,-2)$, $h(3^{-1})$ has a 3-path $(-1,1,3^{-1}2, -3^{-1}2)$. Denote $h(3^{-1})^\lambda$ the cycle obtained from $h(3^{-1})$ inserting λ into the center of this 3-path.

(4) G_D

As $h(1)$ has a 3-path $(\infty,0,1,-1)$, $h(r)$ has a 3-path $(\infty,0,r,-r)$. Denote $h(r)^\lambda$ the cycle obtained from $h(r)$ inserting λ into the center of this 3-path. $h(0)$ has an edge $\{\infty, 3^{-1}2^s\}$. Denote $h(0)^\lambda$ the cycle obtained from $h(0)$ inserting λ into the center of this edge.

Put $H_0 = H_1 \cup H_2 \cup \{3^{-1}\} \cup \{r\}$. Then H_0 is a half-set modulo p, since

$$\{(-2)^i \mid 0 \leq i \leq s-1\} \cup \{3^{-1}2(-2)^i \mid 0 \leq i \leq s-1\}$$

is a half-set, and $(-2)^{s-1} = -r$, $3^{-1}2(-2)^{s-1} = 3^{-1}$.

Proposition 7.2

$$\mathcal{D} = \Sigma(\{h(0)^\lambda\} \cup \{h(a)^\lambda \mid a \in H_0\})$$

is a Dudeney set in K_n.

Proof. Each element of $\mathcal{D}$ is trivially a Hamilton cycle in K_n. The set of all 2-paths in $\Sigma(\{F_0 \cup G^\lambda\} \cup \{h(a) \mid a \in H_0\})$ and the set of all 2-paths in $\mathcal{D}$ are the same. Hence $\mathcal{D}$ has every 2-path in K_n exactly once by Prop. 7.1. Therefore $\mathcal{D}$ is a Dudeney set in K_n. □

Since there is a Dudeney set in K_{p+2} when $p = 17$ [6], we complete the proof of Theorem 1.1.

Finally, we mention the existence of odd prime numbers such that (1) 2 is the square of a primitive root of $GF(p)$, (2) $p \equiv 1 \pmod 4$, and (3) 3 is not a quadratic residue modulo p.

Proposition 7.3 [4, 5] *If we assume the Extended Riemann Hypothesis, there exist infinitly many odd prime numbers satisfying* (1), (2) *and* (3).

8 Example

Put $p = 41$, then $n = 43$ and $r = 20$. We have

$$
\begin{aligned}
h(0) &= (1,-1,-2,2,4,-4,-8,8,\cdots,-20,20,0,\infty,-14,14,7,-7,\cdots,-15,\\
&\quad 13,-13)\\
d &= (1,-2,3,-4,5,-6,7,-8,9,-10,11,-12,13,-14,15,-16,17,-18,\\
&\quad 19,-20;-20,19,-18,17,-16,15,-14,13,-12,11,-10,9,-8,7,\\
&\quad -6,5,-4,3,-2,1)\\
d_1 &= (1,-2,-1,4,-5,6,-7,8,-9,10,-11,12,-13,14,-15,16,-17,18,\\
&\quad -19,20;20,-19,18,-17,16,-15,14,-13,12,-11,10,-9,8,-7,6,\\
&\quad -5,4,-1,-2,1)\\
d_2 &= (1,-2,-1,4,-5,6,-7,8,-9,10,-11,12,-13,-1,15,-16,17,-18,\\
&\quad 19,-20;-20,19,-18,17,-16,15,-1,-13,12,-11,10,-9,8,-7,\\
&\quad 6,-5,4,-1,-2,1)\\
d_3 &= (1,-2,-1,4,1,-6,7,-8,9,-10,11,-12,13,1,-15,16,-17,18,\\
&\quad -19,20;20,-19,18,-17,16,-15,1,13,-12,11,-10,9,-8,7,-6,\\
&\quad 1,4,-1,-2,1)\\
d_4 &= (1,-2,-1,4,1,-6,7,1,-9,10,-11,12,-13,-1,15,-16,17,-18,\\
&\quad 19,-20;-20,19,-18,17,-16,15,-1,-13,12,-11,10,-9,1,7,\\
&\quad -6,1,4,-1,-2,1)\\
h(1) &= (\infty,0,1,-1,-2,2,3,-3,4,5,-4,6,-5,7,-6,-7,8,-8,9,-9,10,\\
&\quad -10,11,-11,12,-12,13,-13,-14,14,-15,15,-16,16,17,-17,\\
&\quad 18,19,-18,-19,20,-20).
\end{aligned}
$$

The following $r+1$ cycles and their rotations by Σ make a Dudeney set in K_n.

$$
\begin{aligned}
&h(0)^\lambda = (\infty,\lambda,-14,14,7,-7,\cdots)\\
&\begin{cases}
h(1)^\lambda = (\infty,0,1,-1,\lambda,-2,2,\cdots)\\
h(-2)^\lambda = (\infty,0,-2,2,\lambda,4,-4,\cdots)\\
h(4)^\lambda = (\infty,0,4,-4,\lambda,-8,8,\cdots)\\
h(-8)^\lambda = (\infty,0,-8,8,\lambda,16,-16\cdots)\\
\cdots\\
h(10)^\lambda = (\infty,0,10,-10,\lambda,-20,20,\cdots)
\end{cases}\\
&\begin{cases}
h(-13)^\lambda = (\infty,0,-13,13,\lambda,-15,15,\cdots)\\
h(-15)^\lambda = (\infty,0,-15,15,\lambda,-11,11,\cdots)\\
\cdots\\
h(-7)^\lambda = (\infty,0,-7,7,\lambda,14,-14,\cdots)
\end{cases}
\end{aligned}
$$

$$h(20)^{\lambda} = (\infty, 0, \lambda, 20, -20, \cdots)$$
$$h(14)^{\lambda} = (\infty, 0, 14, -14, 13, -13, \lambda, 1, -1, \cdots)$$

Acknowledgments The authors would like to thank Professor K. Nakamula and Professor L. Murata for their helpful comments.

References

[1] K. Heinrich, M. Kobayashi and G. Nakamura, Dudeney's Round Table Problem, *Annals of Discrete Math.* **92** (1991) 107-125.

[2] M. Kobayashi, J. Akiyama and G. Nakamura, On Dudeney's round table problem for $p + 2$, submitted.

[3] M. Kobayashi, Kiyasu-Z. and G. Nakamura, A solution of Dudeney's round table problem for an even number of people, *J. Combinatorial Theory* (A) **62** (1993), 26-42.

[4] L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, *Archiev der Mathematik* **57** (1991), 555-565.

[5] L. Murata, Personal communication.

[6] G. Nakamura, Kiyasu-Z. and N. Ikeno, Solution of the round table problem for the case of $p^k + 1$ persons, *Commentarii Mathematici Universitatis Santi Pauli* 29 (1980) 7-20.

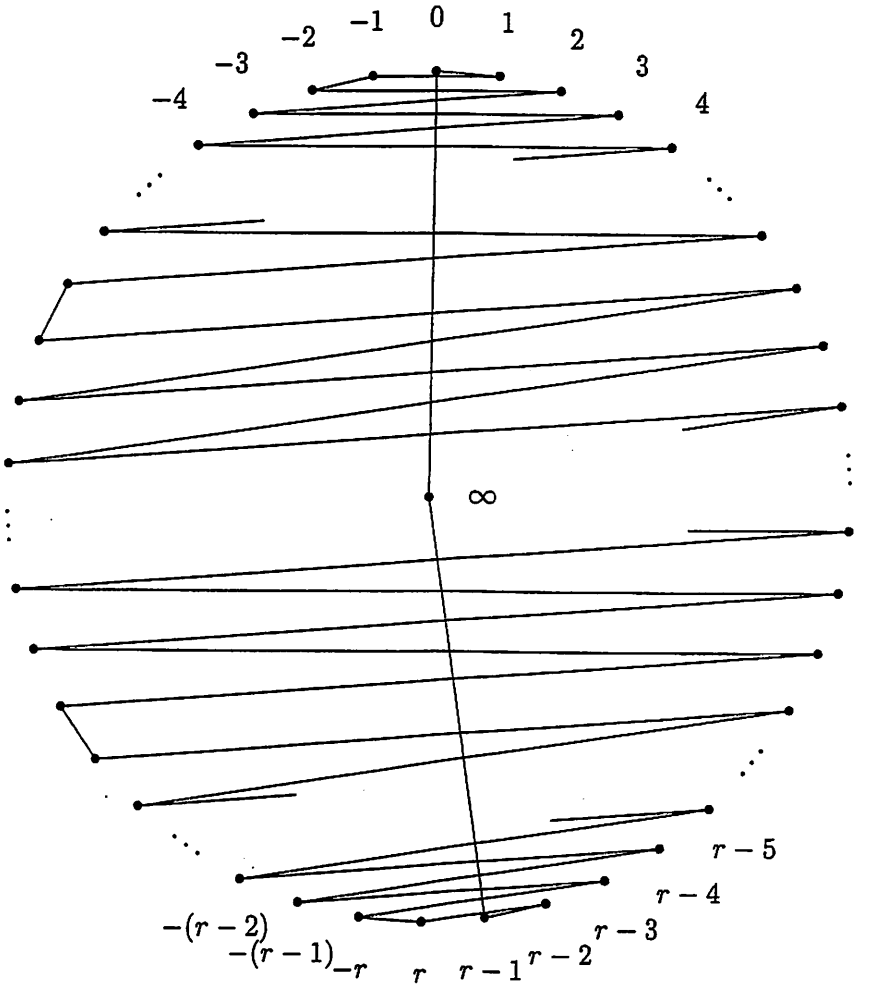

Figure 1: $W(d_2)$

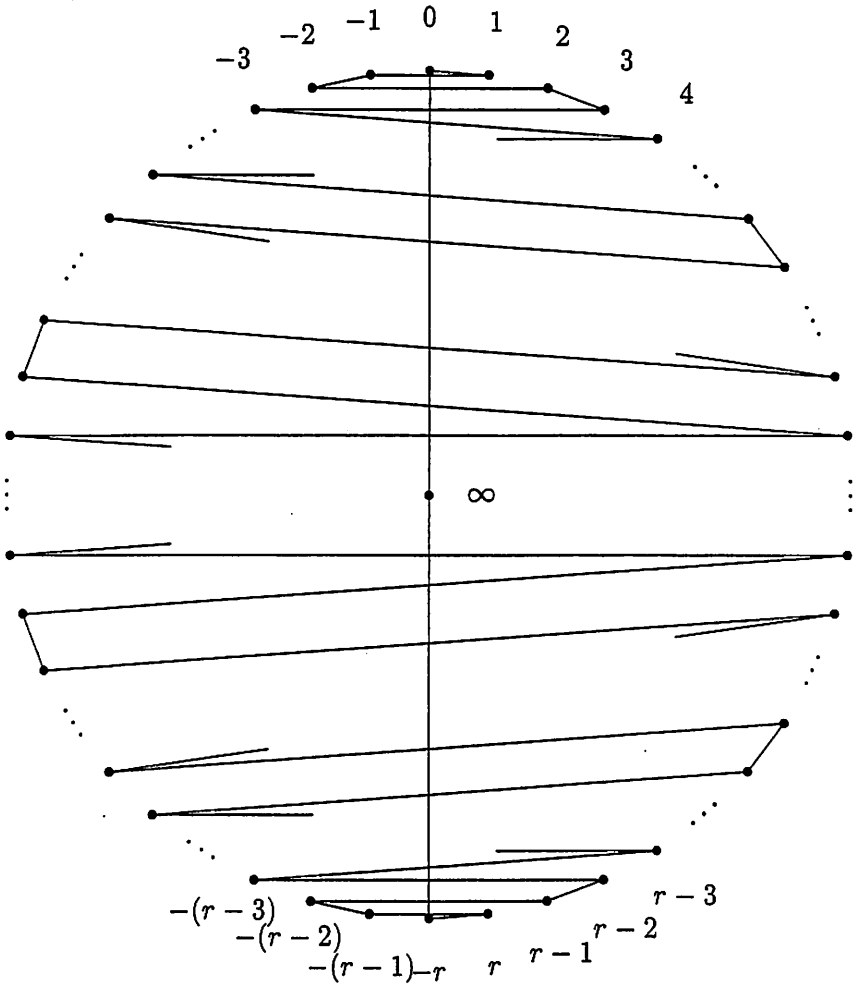

Figure 2: $W(d_4)$ ($b < 8k + 5$ and b is even)

Radio Labelings of Cycles

Ping Zhang [1]
Department of Mathematics and Statistics
Western Michigan University
Kalamazoo, MI 49008 USA

Abstract

A radio labeling of a connected graph G is an assignment of distinct positive integers to the vertices of G, with $x \in V(G)$ labeled $c(x)$, such that

$$d(u,v) + |c(u) - c(v)| \geq 1 + \operatorname{diam} G$$

for every two distinct vertices u, v of G, where $\operatorname{diam} G$ is the diameter of G. The radio number $rn(c)$ of a radio labeling c of G is the maximum label assigned to a vertex of G. The radio number $rn(G)$ of G is $\min\{rn(c)\}$ over all radio labelings c of G. Radio numbers of cycles are discussed and upper and lower bounds are presented.

Key Words: radio labeling, radio number.
AMS Subject Classification: 05C78, 05C12, 05C15.

1 Introduction

For a vertex v of a connected graph G, the *eccentricity* $e(v)$ is the distance between v and a vertex farthest from v. The minimum eccentricity among the vertices of G is the *radius*, *rad* G, and the maximum eccentricity is its *diameter*, *diam* G. A *labeling* of a connected graph is an injection $c : V(G) \to \mathbf{N}$, while a *radio labeling* is a labeling with the added property that

$$d(u,v) + |c(u) - c(v)| \geq 1 + \operatorname{diam} G$$

for every two distinct vertices u, v of G. The *radio number* $rn(c)$ *of a radio labeling* c of G is the maximum label assigned to a vertex of G. The *radio number* $rn(G)$ of G is $\min\{rn(c)\}$ over all radio labelings c of G. A radio labeling c of G is a *minimum radio labeling* if $rn(c) = rn(G)$.

[1] Research supported in part by the Western Michigan University Arts and Sciences Teaching and Research Award Program