Cyclic Hamiltonian cycle systems of the complete graph

Marco Buratti\textsuperscript{a}, Alberto Del Fra\textsuperscript{b}

\textsuperscript{a} Dipartimento di Matematica e Informatica, Università di Perugia, Via Vanvitelli 1, I-06123 Perugia, Italy
\textsuperscript{b} Dipartimento di Metodi e Modelli Matematici per le Scienze Applicate, Università di Roma “La Sapienza”, Via Scarpa 16, I-00161 Roma, Italy

Received 11 November 2002; received in revised form 17 February 2003; accepted 9 June 2003

Dedicated to Lie Zhu on the occasion of his 60th birthday

Abstract

We prove that there exists a cyclic Hamiltonian $k$-cycle system of the complete graph if and only if $k$ is odd but $k \neq 15$ and $p^x$ with $p$ prime and $x > 1$. As a consequence we have the existence of a cyclic $k$-cycle system of the complete graph on $km$ vertices for any pair $(k,m)$ of odd integers with $k$ as above but $(k,m) \neq (3,3)$.

© 2003 Elsevier B.V. All rights reserved.

Keywords: Hamiltonian cycle; Cyclic cycle system; Complete graph

1. Introduction

A $k$-cycle system of a graph $\Gamma=(V,E)$, or $(\Gamma,C_k)$-design (see [8,10,12]), is a set $\mathcal{B}$ of $k$-cycles whose vertices belong to $V$ with the condition that any $\{x,y\} \in E$ is an edge of exactly one cycle of $\mathcal{B}$. Throughout the paper a $k$-trail (so, in particular, a $k$-cycle) whose edges are $\{a_0,a_1\}, \{a_1,a_2\}, \ldots, \{a_{k-1},a_0\}$, will be identified with the $k$-tuple $(a_0,a_1,\ldots,a_{k-1})$ or any cyclic permutation of it. A $k$-cycle system is Hamiltonian if $k = |V|$, and it is cyclic if $V = \mathbb{Z}_v$ and we have $(a_0 + 1,a_1 + 1,\ldots,a_{k-1} + 1) \in \mathcal{B}$ whenever $(a_0,a_1,\ldots,a_{k-1}) \in \mathcal{B}$. A trivial counting shows that the number of cycles of a Hamiltonian cycle system of $K_k$ (the complete graph on $k$ vertices) is $(k-1)/2$. So, a necessary condition for its existence is that $k$ must be odd.

E-mail addresses: buratti@mat.uniroma1.it (M. Buratti), alberto.delfra@uniroma1.it (A. Del Fra).
The condition is also sufficient since, for instance, if \( k = 2h + 1 \) then
\[
\mathcal{B} = \{(\infty, i, i+1, i-1, i+2, i-2, \ldots, i+(h-1), i-(h-1), i+h) | 0 \leq i < h \}
\]
is a Hamiltonian cycle system of the complete graph on \( Z_{k-1} \cup \{\infty\} \). This is an example of 1-rotational Hamiltonian cycle system. Determining the set of values of \( k \) for which there exists a cyclic Hamiltonian cycle system of \( K_k \) is a much more difficult problem. Here we solve this problem by proving the following theorem.

**Theorem 1.1.** There exists a cyclic Hamiltonian cycle system of \( K_k \) if and only if \( k \) is an odd integer but \( k \neq 15 \) and \( k \neq p^z \) with \( p \) a prime and \( z > 1 \).

Once again, as in [4,5], we obtain the above result with the method of partial differences (see [3]).

Throughout the paper whenever we say Hamiltonian \( k \)-cycle (or Hamiltonian \( k \)-cycle system) we understand of the complete graph on \( Z_k \). Also, whenever we speak of a \( k \)-trail, we mean that its vertices are in \( Z_k \).

**Proposition 1.2.** Let \( d \) be a divisor of \( k \) and let \( C = (a_0, a_1, \ldots, a_{k-1}) \) be a \( k \)-trail satisfying the following conditions:

\[
a_k = \sigma(a_d - a_0) + a_\rho \quad \text{for } 0 \leq h < k,
\]

\( \sigma \) and \( \rho \) being quotient and remainder of the Euclidean division of \( h \) by \( d \).

\[
a_d - a_0 = jd \quad \text{with } \gcd(j, k/d) = 1
\]

or, equivalently, \( a_d - a_0 \) is a generator of the subgroup \( S \) of \( Z_k \) of order \( k/d \).

\[
\{a_0, a_1, \ldots, a_{d-1}\} \equiv Z_d \pmod{d}.
\]

Then \( C \) is a Hamiltonian \( k \)-cycle.

**Proof.** By (2)\(_d\), \( S \) is generated by \( a_d - a_0 \) and, by (3)\(_d\), the set \( T = \{a_0, a_1, \ldots, a_{d-1}\} \) is a transversal of \( S \) in \( Z_k \). Observing that, by (1)\(_d\), the elements of \( C \) are precisely those of the form \( s + t \) with \( (s, t) \in S \times T \), any element of \( Z_k \) appears in \( C \). The assertion follows.

Any Hamiltonian \( k \)-cycle \( C = (a_0, a_1, \ldots, a_{k-1}) \) trivially satisfies conditions (1)\(_k\), (2)\(_k\) and (3)\(_k\) (understanding that \( a_k = a_0 \)) so that the following definition makes sense.

**Definition 1.3.** The cotype \( \tau(C) \) of a Hamiltonian \( k \)-cycle \( C = (a_0, a_1, \ldots, a_{k-1}) \) is the least divisor \( d \) of \( k \) such that (1)\(_d\)–(3)\(_d\) hold.

Equivalently, one could check that \( \tau(C) \) is the least divisor \( d \) of \( k \) such that \( C + d = C \) so that \( \{C, C+1, \ldots, C+d-1\} \) is the orbit of \( C \) under \( Z_k \).

We prefer to speak of cotype rather than type since in [4,5] the type \( \alpha(C) \) of a cycle \( C \) with vertices in \( Z_v \) is the order its stabilizer under \( Z_v \).
Note that if \( C \) is a Hamiltonian \( k \)-cycle and \( d \) is a divisor of \( k \) such that \( C + d = C \), then \( \tau(C) \) is a divisor of \( d \). In fact, \( C + d = C \) implies that the subgroup of \( \mathbb{Z}_k \) of order \( k/d \) is a subgroup of the stabilizer of \( C \) under \( \mathbb{Z}_k \). It follows, by the Theorem of Lagrange, that \( k/d \) divides \( k/\tau(C) \), i.e., \( \tau(C) \) divides \( d \).

We give some examples in order to clarify the concept of cotype. Consider the following Hamiltonian 15-cycles:

\[
A = (0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11);
\]

\[
B = (0, 2, 7, 3, 5, 10, 6, 8, 13, 9, 11, 1, 12, 14, 4);
\]

\[
C = (0, 1, 8, 12, 4, 10, 11, 3, 7, 14, 5, 6, 13, 2, 9).
\]

We have

\[
A + 1 = (1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12) = A
\]

so that \( \tau(A) = 1 \). We also have

\[
B + 3 = (3, 5, 10, 6, 8, 13, 9, 11, 1, 12, 14, 4, 0, 2, 7) = B;
\]

\[
C + 5 = (5, 6, 13, 2, 9, 0, 1, 8, 12, 4, 10, 11, 3, 7, 14) = C.
\]

Then, since \( B + 1 \neq B \) and \( C + 1 \neq C \), we may claim that \( \tau(B) = 3 \) and \( \tau(C) = 5 \).

**Notation 1.4.** Throughout the paper, given a divisor \( d \) of \( k \), we will denote by \( [a_0, a_1, \ldots, a_d]_k \) the \( k \)-trail \( (a_0, a_1, \ldots, a_k) \) satisfying condition (1). Hence, explicitly, setting \( \delta = a_d - a_0 \):

\[
[a_0, a_1, \ldots, a_d]_k = (a_0, a_1, \ldots, a_{d-1}, \delta + a_0, \delta + a_1, \ldots, \delta + a_{d-1}, \ldots),
\]

\[
(k/d - 1)\delta + a_0, (k/d - 1)\delta + a_1, \ldots, (k/d - 1)\delta + a_{d-1}.
\]

Using this notation the 15-cycles \( A, B, \) and \( C \) given before may be shortly presented as

\[
A = [0, 4]_{15}; \quad B = [0, 2, 7, 3]_{15}; \quad C = [0, 1, 8, 12, 4, 10]_{15}.
\]

Given a Hamiltonian \( k \)-cycle \( A = (a_0, a_1, \ldots, a_{k-1}) \), its list of partial differences is the multiset \( \partial A = \pm \{a_{i+1} - a_i \mid 0 \leq i < d \} \) of size \( 2d \) where \( d = \tau(A) \). More generally, given a set \( \mathcal{F} = \{A_1, \ldots, A_n\} \) of Hamiltonian \( k \)-cycles, the list of partial differences from \( \mathcal{F} \) is defined by \( \partial \mathcal{F} = \bigcup_{i=1}^n \partial A_i \) where the union has to be understood between multisets (elements have to be counted with their respective multiplicities).

As an example, consider again the Hamiltonian 15-cycles \( A, B, \) \( C \) we gave above. We have:

\[
\partial A = \{\pm 4\}; \quad \partial B = \{\pm 2, \pm 5, \pm 4\}; \quad \partial C = \{\pm 1, \pm 7, \pm 4, \pm 7, \pm 6\};
\]

\[
\partial \{A, B, C\} = \{\pm 1, \pm 2, \pm 4, \pm 4, \pm 4, \pm 5, \pm 6, \pm 7, \pm 7\}.
\]
For presenting a cyclic Hamiltonian \(k\)-cycle system, it suffices to give a set of base cycles of it, i.e., a complete system of representatives for its cycle-orbits under \(\mathbb{Z}_k\). As a particular consequence of the theory developed in [3] we have:

**Proposition 1.5.** A set \(\mathcal{F}\) of Hamiltonian \(k\)-cycles is the set of base cycles of a cyclic Hamiltonian \(k\)-cycle system if and only if \(\partial \mathcal{F} = \mathbb{Z}_k - \{0\}\).

Also here, it is appropriate to give an example. Consider the Hamiltonian 21-cycles \(A = [0, 2, 1, 15]_{21}\) of cotype 3 and \(B = [0, 6, 15, 12, 11, 3, 14]_{21}\) of cotype 7. We have

\[
\partial A = \{\pm 2, \pm 1, \pm 7\}; \quad \partial B = \{\pm 6, \pm 9, \pm 3, \pm 4, \pm 5, \pm 8, \pm 10\}
\]

and hence \(\partial \{A, B\} = \mathbb{Z}_{21} - \{0\}\). Thus, by Proposition 1.5, \(\{A, B\}\) is the set of base cycles of a cyclic Hamiltonian 21-cycle system. We explicitly display this cycle system below.

\[
A = (0, 2, 1, 15, 17, 16, 9, 11, 10, 3, 5, 4, 18, 20, 19, 12, 14, 13, 6, 8, 7),
\]

\[
A + 1 = (1, 3, 2, 16, 18, 17, 10, 12, 11, 4, 6, 5, 19, 0, 20, 13, 15, 14, 7, 9, 8),
\]

\[
A + 2 = (2, 4, 3, 17, 19, 18, 11, 13, 12, 5, 7, 6, 20, 1, 0, 14, 16, 15, 8, 10, 9),
\]

\[
B = (0, 6, 15, 12, 16, 11, 3, 14, 20, 8, 5, 9, 4, 17, 7, 13, 1, 19, 2, 18, 10),
\]

\[
B + 1 = (1, 7, 16, 13, 17, 12, 4, 15, 0, 9, 6, 10, 5, 18, 8, 14, 2, 20, 3, 19, 11),
\]

\[
B + 2 = (2, 8, 17, 14, 18, 13, 5, 16, 1, 10, 7, 11, 6, 19, 9, 15, 3, 0, 4, 20, 12),
\]

\[
B + 3 = (3, 9, 18, 15, 19, 14, 6, 17, 2, 11, 8, 12, 7, 20, 10, 16, 4, 1, 5, 0, 13),
\]

\[
B + 4 = (4, 10, 19, 16, 20, 15, 7, 18, 3, 12, 9, 13, 8, 0, 11, 17, 5, 2, 6, 1, 14),
\]

\[
B + 5 = (5, 11, 20, 17, 0, 16, 8, 19, 4, 13, 10, 14, 9, 1, 12, 18, 6, 3, 7, 2, 15),
\]

\[
B + 6 = (6, 12, 0, 18, 1, 17, 9, 20, 5, 14, 11, 15, 10, 2, 13, 19, 7, 4, 8, 3, 16).
\]

The only if part of Theorem 1.1 is quite easy.

**“Only if” part” of Theorem 1.1:** We have to prove that for \(k = 15\) or \(k = p^x\) with \(p\) a prime and \(x > 1\), no cyclic Hamiltonian \(k\)-cycle system exists.

Observe, first, that if \(\mathcal{B}\) is a cyclic Hamiltonian \(k\)-cycle system then no cycle of \(\mathcal{B}\) is of cotype \(k\) since in the opposite case \(\mathcal{B}\) would contain the whole orbit under \(\mathbb{Z}_k\) of such a cycle and hence we would have \((k - 1)/2 = |\mathcal{B}| > k\) that is absurd.

Assume that \(\mathcal{F}\) is the set of base cycles of a cyclic 15-cycle system so that, by Proposition 1.5, \(\partial \mathcal{F} = \mathbb{Z}_{15} - \{0\}\). Let \(A\) be the cycle of \(\mathcal{F}\) admitting 5 as a partial difference, and let \(\tau(A) = d\) so that conditions (2)_d and (3)_d hold. It is easily seen this is possible only for \(d = 15\) or \(d = 3\) but we must exclude \(d = 15\) for what commented above. Thus, \(\tau(A) = 3\) and \(\partial A\) has size 6.
Analogously, if $B$ is the cycle of $F$ admitting 3 as a partial difference, then $\tau(B) = 5$ so that $|\partial B| = 10$. It follows that $\partial F$ has size at least 16, a contradiction.

Now let $k = p^x$ with $p$ a prime and $x > 1$. In view of what observed before, the non-existence of a cyclic Hamiltonian $k$-cycle system is proved if we show that a Hamiltonian $k$-cycle $C$ admitting $p^{x-1}$ as a partial difference is necessarily of cotype $k$. In the opposite case we would have $\tau(C) = p^\beta$ with $1 \leq \beta \leq x-1$ ($\beta \neq 0$ otherwise $\partial C = \{ \pm w \}$ for some unit $w$ of $Z_k$). By (3) $p^\rho$, the elements $a_0, a_1, \ldots, a_{p^\rho - 1}$ are pairwise distinct modulo $p^\beta$ and, by (2) $p^\rho$, we have $a_{i+1} \equiv a_i (mod p^\beta)$. So we have $a_{i+1} - a_i \neq 0 (mod p^\beta)$ for $0 \leq i < p^\beta$. Considering that $p^\beta$ is a divisor of $p^{x-1}$, this implies that no partial difference from $C$ is equal to $p^{x-1}$, a contradiction.

Our main result will be the if part of Theorem 1.1.

2. Some auxiliary lemmas

We will often identify the ring $Z_k$ of residues mod $k$ with a direct sum $Z_{h_1} \oplus \cdots \oplus Z_{h_t}$ where the $h_i$’s are mutually coprime integers such that $h_1 h_2 \cdots h_t = k$. The set of units and the set of zero divisors of the ring $Z_n$ will be denoted by $U(Z_n)$ and $D(Z_n)$, respectively. Also, we set $Z_n^* = Z_n - \{0\}$.

We need the following lemmas.

Lemma 2.1. Let $k$ be an odd integer with at least two prime factors. Let $q = p^x > 3$ be a factor in the prime power factorization of $k$ and let us identify $Z_k$ with $Z_q \oplus Z_{k/q}$. Then there exists a Hamiltonian $k$-cycle $A$ such that $\partial A \cap D(Z_k) = Z_q^* \times \{0\}$ and $\partial A \cap U(Z_k)$ is a $(q + 1)$-set (not multiset!) of units of the form $\pm(x, 1)$ with $x \neq 1$.

Proof. Take the $k$-trail $A = [a_0, a_1, \ldots, a_q]_k$ with

$$a_h = (((-1)^h[h/2], 0) \text{ for } h \leq (q - 1)/2$$

and the $a_h$’s with $(q - 1)/2 < h \leq q$ defined as follows:

Case 1: $p \equiv 1 (mod 4)$.

$$a_h = \begin{cases} 
(\frac{h}{2}, 0) & \text{for } h \text{ even}, \\
(\frac{h + (-1)^{h/p}}{2}, -1) & \text{for } h \text{ odd, } h \not\equiv p (mod 2p), \\
(\frac{h + p}{2}, 1) & \text{for } q \not\equiv h \equiv p (mod 2p);
\end{cases}$$

$$a_q = (0, -1).$$
Case 2: $p \equiv 3 \pmod{4}$ and $\alpha$ is odd.

$$a_h = \begin{cases} 
\left( \frac{h}{2}, 1 \right) & \text{for } h \text{ even } < q - 1, \\
\left( -\frac{h + (-1)^{[h/p]}}{2}, 0 \right) & \text{for } h \text{ odd } < q - 2, h \not\equiv p \pmod{2p}, \\
\left( -\frac{h + p}{2}, 0 \right) & \text{for } q - h \equiv p \pmod{2p};
\end{cases}$$

$$a_{q-2} = \left( \frac{1 - q}{2}, 0 \right); \quad a_{q-1} = \left( \frac{q - 1}{2}, 3 \right); \quad a_{q} = (0, 2).$$

Case 3: $p \equiv 3 \pmod{4}$ and $\alpha$ is even.

$$a_h = \begin{cases} 
\left( -\frac{h + 1}{2}, 1 \right) & \text{for } h \text{ odd } < q - 2, \\
\left( h + 1 + (-1)^{[h/p]} \right) & \text{for } h \text{ even } < q - 2, h \not\equiv p - 1 \pmod{2p}, \\
\left( h + 1 - p \right) & \text{for } q - 1 \not\equiv p - 1 \pmod{2p};
\end{cases}$$

$$a_{q-2} = \left( \frac{q - p}{2}, 1 \right); \quad a_{q-1} = \left( \frac{1 - q}{2}, 0 \right); \quad a_{q} = (0, -1).$$

One may check that, in each case, $A$ is a Hamiltonian $k$-cycle of cotype $q$ satisfying the required condition.

Consider, for instance, the 1st case.

Obviously, $a_{q} = (0, -1)$ is a generator of the subgroup of order $k/q$ so that, since $a_{0} = (0, 0)$, $A$ satisfies condition $(2)_q$.

For $0 \leq h \leq q - 1$, let $a'_h$ be the 1st coordinate of $a_h$. Observing that $\lfloor 2i/p \rfloor$ and $\lfloor (2i - (1)^{[2i/p]}/p \rfloor$ have the same parity for $i \not\equiv 0 \pmod{p}$, one may check that for any $i \in \{1, \ldots, (q - 1)/2\}$ the following identities hold:

$$i = a'_{2i} \quad \text{and} \quad -i = \begin{cases} 
 a'_{2i-1} & \text{if } i \leq (q - 1)/4, \\
 a'_{2i-(1)^{[2i/p]}} & \text{if } (q - 1)/4 < i \not\equiv 0 \pmod{p}, \\
 a'_{2i-p} & \text{if } (q - 1)/4 < i \equiv 0 \pmod{p}.
\end{cases}$$

Then, since we have $a'_0 = 0$, we may claim that $\{a'_0, a'_1, \ldots, a'_{q-1}\} = \{0, \pm 1, \pm 2, \ldots, \pm(q-1)/2\}$. This assures that $A$ also satisfies condition $(3)_q$. Hence, by Proposition 1.2, $A$ is a Hamiltonian $k$-cycle and, by Definition 1.3, $\tau(A)$ is a divisor of $q$. If $\tau(A) \neq q$, then $\tau(A) = p^\beta$ with $\beta < \alpha$. By $(1)_{p^\alpha}$, we would have $a_{p^\beta+1} = a_1 + a_{p^\beta}$ but this is easily seen to be false. Thus $A$ is actually a Hamiltonian $k$-cycle of cotype $q$. 
We are sure that \( A \) satisfies the required condition if we prove that \( \partial A \) is disjoint union of the sets

\[
L = \mathbb{Z}_q^* \times \{0\};
\]

\[
M = \{\pm(i,1) \mid (q-1)/2 \leq i \leq q-1; i \neq 0 \text{ (mod } p)\} ;
\]

\[
N = \{\pm(i,1) \mid i = 2jp - (p \pm 1)/2; 1 \leq j \leq (q-p)/4p\}.
\]

Since \( L, M, N \) are obviously disjoint and the sum of their sizes is exactly equal to the size 2q of \( \partial A \), it is enough to show that any element of \( L \cup M \cup N \) appears in \( \partial A \).

Setting \( q = 4n+1 \), we see that \( a_0, a_1, \ldots, a_{(q−1)/2} \) are, respectively,

\[
(0,0), (−1,0), (1,0), (−2,0), (2,0), \ldots, (−n,0), (n,0)
\]

so that the partial differences \( \pm(a_{i+1}−a_i) \) with \( 0 \leq i < (q−1)/2 \) are

\[
(±1,0), (±2,0), (±3,0), (±4,0), \ldots, (±2n,0),
\]

namely, just the elements of \( L \).

Now observe that the element \( ((q−1)/2,1) \in M \) is obtainable as difference \( a_{q−1}−a_q \).

For any other \( (i, 1) \in M \) we have

\[
(i, 1) = (−1)^i(a_i−a_{−(−1)^i/p}).
\]

The above equality may be easily checked distinguishing the four possible cases according to the parity of \( i \) and \( [i/p] \).

Consider, finally, an element \( (i, 1) \in N \) so that \( i = 2jp - (p \pm 1)/2 \) with \( 1 \leq j \leq (q-p)/4p \). One may check that \( (i, 1) = a_{−2jp}−a_{−2jp±1} \).

The other two cases may be treated similarly. \( \square \)

**Lemma 2.2.** Let \( \phi \) be the Euler totient function and let \( k \) be an odd integer with prime power factorization \( k = q_1q_2\ldots q_n, \; q_i = p_i^{n_i}, \; 3 \leq p_1 < p_2 < \cdots < p_n. \) Set

\[
\psi(k) = 1 + \sum_{i=1}^{n-1} (q_i + q_1q_2\ldots q_i) + q_n + \phi \left( \frac{k}{q_{n-1}q_n} \right) \frac{q_{n-1}}{p_{n-1}} \left( \frac{q_n}{p_n} - 1 \right) - \phi(q_1\ldots q_{n-1}).
\]

Then, if \( n \geq 2 \) and \( k \neq 15 \) we have \( \psi(k) \leq \phi(k) \).

**Proof.** The assertion may be obtained by induction on \( n \) proving the following three cases.

**Case 1:** \( n = 2 \).

We have to prove that if \( q_1q_2 \neq 15 \) then

\[
1 + \frac{q_1q_2}{p_1p_2} + q_1 + q_2 \leq \phi(q_1q_2).
\]

Note that \( \phi(q_1) = q_1 - q_1/p_1 \geq 2q_1/3 \) since \( p_1 \geq 3 \) and that \( \phi(q_2) = q_2 - q_2/p_2 \geq 4q_2/5 \) since \( p_2 \geq 5 \). Thus we have \( \phi(q_1q_2) \geq 8q_1q_2/15 \).
Also note that $1+q_1q_2/(p_1p_2)+q_1 \leq 4q_1/3+q_1q_2/15$ since $q_1/3 \geq 1$ and $p_1p_2 \geq 15$.

So (4) certainly holds if $4q_1/3+q_2 \leq 7q_1q_2/15$ that may be rewritten as $q_1 \geq 15q_2/(7q_2-20)$ or $q_2 \geq 20q_1/(7q_1-15)$.

Both the real functions $f_1(x)=15x/(7x-20)$ and $f_2(x)=20x/(7x-15)$ are decreasing so that, being $q_1 \geq 3$ and $q_2 \geq 5$, we have $15q_2/(7q_2-20) \leq f_1(5)=5$ and $20q_1/(7q_1-15) \leq f_2(3)=10$. It follows that (4) holds for $q_1 \geq 5$ or $q_2 \geq 11$. In the only remaining case where $(q_1,q_2)=(3,7)$ condition (4) may be checked directly.

Case 2: $n=3$; $q_1=3$; $q_2=5$.

In this case $\psi(k) \leq \phi(k)$ becomes $17+q_3+2q_3/p_3 \leq 8(q_3-q_3/p_3)$ that is obvious since $p_3 \geq 7$.

Case 3: $n \geq 3$ and $\psi(k/q_n) \leq \phi(k/q_n)$.

Note, first, that $\phi(k/q_n) \geq 8$ and $p_n \geq 7$. We obviously have

$$\psi(k) < \psi\left(\frac{k}{q_n}\right) + \frac{k}{q_n} + \phi\left(\frac{k}{q_n}\right) \left(\frac{q_{n-1}}{p_{n-1}}\right) \left(\frac{q_n}{p_n} - 1\right) + q_n. \tag{5}$$

From $\phi(k/q_n)=((p_1-1)(q_1/p_1)(p_2-1)(q_2/p_2)\cdots(p_{n-1}-1)(q_{n-1}/p_{n-1})$ and $p_1-1 \geq 2$, $p_2-1 > p_1$, ..., $p_{n-1}-1 > p_{n-2}$, we get $p_{n-1}\phi(k/q_n) > 2q_1q_2\cdots q_{n-1} = 2k/q_n$ and hence

$$\frac{k}{q_n} < \frac{p_{n-1}}{2} \phi\left(\frac{k}{q_n}\right). \tag{6}$$

Also, since $q_{n-1}/p_{n-1} < \phi(q_{n-1})$, we have

$$\phi\left(\frac{k}{q_n}\right) \left(\frac{q_{n-1}}{p_{n-1}}\right) \left(\frac{q_n}{p_n} - 1\right) < \phi\left(\frac{k}{q_n}\right) \left(\frac{q_n}{p_n} - 1\right). \tag{7}$$

Inequalities (5)-(7) together with the hypothesis $\psi(k/q_n) \leq \phi(k/q_n)$ give

$$\psi(k) < \phi\left(\frac{k}{q_n}\right) \left(\frac{p_{n-1}}{2} + \frac{q_n}{p_n}\right) + q_n.$$

If $\psi(k) > \phi(k)$ we would have $q_n > \phi(k/q_n)(\phi(q_n) - (p_n-1)/2 - q_n/p_n)$. It would follow $p_n q_n^2 > 8(p_n^2 - 2p_n^{n-1} - p_n/2)$ and hence $7p_n < 16 + 4p_n/p_n^{n-1} \leq 16 + 4p_n$ that implies $p_n \leq 5$, a contradiction. $\square$

3. The main result

We are now able to prove our main result. Sometimes in the proof we will use the following notation.

**Notation 3.1.** Given $T \subset Z_n$, we set $T^+ = T \cap \{0,1,2,\ldots,\lfloor n/2 \rfloor\}$.

“*If part* of Theorem 1.1: As observed in [6], if $k$ is a prime then $\{(0, i, 2i, 3i, \ldots, (k-1)i) | 1 \leq i \leq (k-1)/2\}$ is a cyclic Hamiltonian $k$-cycle system.
In the following we will assume that \( k > 15 \) is an odd integer with at least two prime factors and prime power factorization \( k = q_1 q_2 \cdots q_n \) with \( q_i = p_i^{n_i} \), \( p_i \) prime, and \( 3 \leq p_1 < p_2 < \cdots < p_n \).

We show, first, that identifying \( Z_k \) with \( Z_{q_1} \oplus Z_{q_2} \oplus \cdots \oplus Z_{q_n} \), there exists a set \( \mathcal{F}_0 = \{ A_1, \ldots, A_n \} \) of Hamiltonian \( k \)-cycles such that

\[
\tilde{\mathcal{F}}_0 = D_0 \cup U_0,
\]

where \( D_0 \) is the set of zero divisors of the form \( \pm(0,0,\ldots,0,x_i,0,0,\ldots,0) \) for some \( i \) and some \( x_i \in Z_{q_i}^* \), and \( U_0 \) is a \( (n + q_1 + \cdots + q_n) \)-set (not multiset!) of units of the form \( \pm(1,1,\ldots,1,x_i,1,1,\ldots,1) \) for some \( i \) and some \( x_i \in U(Z_{q_i}) \).

Assume that \( q_1 > 3 \). Applying Lemma 2.1 with \( q = q_i \), we may find a Hamiltonian \( k \)-cycle \( A_i \) such that \( \tilde{c}A_i \cap D(Z_k) = \{ 0 \} \times \cdots \times \{ 0 \} \times Z_{q_i}^* \times \{ 0 \} \times \cdots \times \{ 0 \} \) and \( \tilde{c}A_i \cap U(Z_k) \) is a \( (q_i + 1) \)-set whose elements are of the form \( \pm(1,1,\ldots,1,x_i,1,1,\ldots,1) \) with \( x_i \in U(Z_{q_i}) - \{ 1 \} \). It follows that for \( n > 2 \) the set \( \mathcal{F}_0 = \{ A_1, \ldots, A_n \} \) satisfies the required condition since \( \tilde{c}A_i \cap \tilde{c}A_j \) have empty intersection whenever \( i \neq j \).

Instead, in the case of \( n=2 \) we may possibly have \( (1,-1) \in \tilde{c}A_1 \cap \tilde{c}A_2 \). We may overcome this inconvenience by replacing \( A_2 \) with \( (-1,1) \cdot A_2 \), that is the cycle obtainable from \( A_2 \) by multiplying all its vertices by \( (-1,1) \).

If \( q_1 = 3 \), take \( A_1 \) of cotype 3 defined by

\[
A_1 = [(0,0,0,\ldots,0),(1,0,0,\ldots,0),(-1,1,1,\ldots,1),(0,-1,2,\ldots,2)],
\]

and, for \( i > 1 \), construct \( A_i \) as in the above case. Also here one may easily check that \( \mathcal{F}_0 = \{ A_1, \ldots, A_n \} \) satisfies the required condition (in the case of \( n = 2 \) too).

Now, let us write \( Z_k \) as \( Z_k = Z_{k(q_1-1)q_2} \oplus Z_{q_1-1} \oplus Z_{q_2} \) and, for any fixed pair \( (u,z) \in U(Z_{k(q_1-1)q_2}) \times D(Z_{q_2}) \), let \( B_{u,z} \) be the \( k \)-trail defined by \( B_{u,z} = [b_{u,z,0}, b_{u,z,1}, \ldots, b_{u,z,q_{n-1}}]_k \) where

\[
b_{u,z,h} = \begin{cases} 
(0, -h, 0) & \text{for } h \text{ even,} \\
(u, h + (-1)^{\lfloor h/p_{n-1} \rfloor}z/2, z) & \text{for } h \text{ odd, } h \not\equiv p_{n-1} \pmod{2p_{n-1}}, \\
(u, h + p_{n-1}/2, z + 1) & \text{for } q_{n-1} \not\equiv h \equiv p_{n-1} \pmod{2p_{n-1}};
\end{cases}
\]

\[
b_{u,z,q_{n-1}} = (u, 0, z - 1).
\]

Note, first, that \( z \in D(Z_{q_2}) \) implies that \( z - 1 \in U(Z_{q_2}) \) so that \( b_{u,z,q_{n-1}} \) is a generator of the subgroup of order \( k/q_{n-1} \) and hence, considering that \( B_{u,z,0} = (0,0,0) \), \( B_{u,z} \) satisfies condition (2) \( q_{n-1} \). Reasoning as in the proof of Lemma 2.1, we see that the 2nd coordinates of the elements \( b_{u,z,0}, b_{u,z,1}, \ldots, b_{u,z,q_{n-1}-1} \) are \( \{0, \pm1, \pm2, \ldots, \pm(q_{n-1} - 1)/2\} \). This assures that \( B_{u,z} \) also satisfies condition (3) \( q_{n-1} \). So, by Proposition 1.2, \( B_{u,z} \) is a Hamiltonian \( k \)-cycle and, by Definition 1.3, its cotype is a divisor of \( q_{n-1} \). Also here, reasoning as in the proof of Lemma 2.1, we can see that \( B_{u,z} \) is actually of cotype \( q_{n-1} \).
We may check that:
\[ b_{u,z,q_{n-1}} - b_{u,z,q_{n-1}} - 1 = (u, (q_{n-1} - 1)/2, z - 1); \]
\[ (u, i, z) = (-1)^{i+1}(b_{u,z,i} - b_{u,z,i - (1)^{u/Z_n}}) \quad \forall i \in U(Z_{q_{n-1}}); \]
\[ (u, 2j p_{n-1} - (p_{n-1} \pm 1)/2, z + 1) = b_{u,z,(2j-1)p_{n-1}} - b_{u,z,(2j-1)p_{n-1} \pm 1} \]
for \( 1 \leq j \leq (q_{n-1} - p_{n-1})/(2 p_{n-1}). \)

From the above identities we have that \( \partial B_{u,z} \) contains:
- \( \pm(u, (q_{n-1} - 1)/2, z - 1); \)
- all elements of the form \( \pm(u, i, z) \) with \( i \in U(Z_{q_{n-1}}); \)
- all elements of the form \( \pm(u, 2j p_{n-1} - (p_{n-1} \pm 1)/2, z + 1) \) with \( 1 \leq j \leq (q_{n-1} - p_{n-1})/(2 p_{n-1}). \)

An easy computation shows that the total number of elements listed above is \( 2 q_{n-1} \), that is the size of \( \partial B_{u,z}. \) We conclude that no other element appears in \( \partial B_{u,z}. \) Hence we have
\[ \partial B_{u,z} \cap D(Z_k) = \pm\{u\} \times U(Z_{q_{n-1}}) \times \{z\}; \]
\[ \partial B_{u,z} \cap U(Z_k) = \pm\{(u, (q_{n-1} - 1)/2, z - 1)\} \cup \]
\[ \pm\{(u, 2j p_{n-1} - (p_{n-1} \pm 1)/2, z + 1) | 1 \leq j \leq (q_{n-1} - p_{n-1})/(2 p_{n-1})\}. \]

In view of this, setting
\[ \mathcal{F}_1 = \{B_{u,z} | (u, z) \in U(Z_k/(q_{n-1}q_n)) \times D(Z_{q_n})^+\}, \]
(for the meaning of \( D(Z_{q_n})^+ \) see Notation 3.1) we have
\[ \partial \mathcal{F}_1 = D_1 \cup U_1, \quad (9) \]
where \( D_1 = U(Z_k/(q_{n-1}q_n)) \times U(Z_{q_{n-1}}) \times D(Z_{q_n}) \) and \( U_1 \) is a set of units of \( Z_k. \)

We point out that \( U_1 \) is actually a set (not multiset) and that \( U_0 \cap U_1 = \emptyset. \) This may be easily seen looking at the form of \( \partial B_{u,z}. \)

Note that \( \mathcal{F}_1 \) is empty when \( q_n \) is prime since in this case we have \( D(Z_{q_n}) = \emptyset. \)

Now, for \( i = 2, \ldots, n \) write \( Z_k^i \) as \( Z_k = Z_{q_1 \cdots q_{i-1}} \oplus Z_{q_i} \oplus Z_k/(q_1 \cdots q_{i-1}) \) and set
\[ X_i = Z_{q_1 \cdots q_{i-1}}^i \quad \text{for} \quad 2 \leq i \leq n - 1; \]
\[ X_n = D(Z_{q_1 \cdots q_{n-1}}). \]

Choose a \( |X_i| \)-subset \( U_i \) of \( U(Z_k) \) with the conditions that \( u \in U_i \Leftrightarrow -u \in U_i, \) and that \( U_0, U_1, U_2, \ldots, U_n \) are pairwise disjoint. Since we have already seen that \( U_0 \cap U_1 = \emptyset, \) this
choice is possible provided that \(|U_0| + |U_1| + \sum_{i=2}^{n} |X_i| \leq |U(Z_k)|\) and this is what Lemma 2.2 assures. We may see it considering that the following equalities hold:

\[
|U_0| = n + q_1 + \cdots + q_n; \quad |U_1| = \phi \left( \frac{k}{q_{n-1}q_n} \right) \frac{q_{n-1}}{p_{n-1}} \left( \frac{q_n}{p_n} - 1 \right);
\]

\[
|U(Z_k)| = \phi(k);
\]

\[
|X| = q_1q_2 \cdots q_{i-1} - 1 \quad \text{for } 2, \ldots, n - 1;
\]

\[
|X_n| = q_1q_2 \cdots q_{n-1} - \phi(q_1q_2 \cdots q_{n-1}) - 1.
\]

Construct, arbitrarily, a bijection \(f_i : x \in X_i^+ \rightarrow u_x = (r_x, s_x, t_x) \in U_i^+\) and, for each \(x \in X_i^+\), set:

\[
C_x = \{(0, 0, 0), (x, 2s_x, 0), (0, -2s_x, 0), (x, 4s_x, 0), (0, -4s_x, 0), (x, 6s_x, 0), (0, -6s_x, 0), \ldots, (x, (q_i - 1)s_x, 0), (0, -(q_i - 1)s_x, 0), (-r_x, 0, -t_x)\}_i.
\]

Obviously, \((-r_x, 0, -t_x)\) is a generator of the subgroup of order \(k/q_i\) and hence \(C_x\) satisfies condition (2)\(_q_i\). Also, since \(2s_x\) is a unit of \(Z_{q_i}\), we see that the 2nd coordinates of the first \(q_i\) vertices of \(C_x\) are pairwise distinct modulo \(q_i\) so that \(C_x\) satisfies condition (3)\(_q_i\). Hence, by Proposition 1.2, \(C_x\) is a Hamiltonian \(k\)-cycle and, by Definition 1.3, \(\tau(C_x)\) divides \(q_i\). Reasoning, again, as in Lemma 2.1, we may see that \(C_x\) is actually of cotype \(q_i\).

Note that \(u_x\) and \(-u_x\) appear among the partial differences of \(C_x\) since we have:

\[
(0, -(q_i - 1)s_x, 0) - (-r_x, 0, -t_x) = (r_x, s_x, t_x) = u_x.
\]

The other partial differences from \(C_x\) are

\[
\pm(x, 2s_x, 0), \pm(x, 4s_x, 0), \pm(x, 6s_x, 0), \pm(x, 8s_x, 0), \ldots, \pm(x, 2(q_i - 1)s_x, 0),
\]

namely, all elements of the form \(\pm(x, 2hs_x, 0)\) with \(1 \leq h \leq (q_i - 1)/2\). On the other hand, being \(2s_x\) a unit of \(Z_{q_i}\), we have \(\{\pm 2hs_x \mid 1 \leq h \leq (q_i - 1)/2\} = Z_{q_i}^*\). Thus we may write:

\[
\partial C_x = (\{x, -x\} \times Z_{q_i}^* \times \{0\}) \cup \{u_x, -u_x\}.
\]

In view of the above formula, setting

\[
\mathcal{F}_i = \{C_x \mid x \in X_i^+\},
\]

we have

\[
\partial \mathcal{F}_i = D_i \cup U_i
\]

where \(D_i = Z_{q_i-1,q_i-2}^* \times Z_{q_i}^* \times \{0\}\) for \(2 \leq i < n\), while \(D_n = D(Z_{q_1,q_2-1}) \times Z_{q_n}^*\).

Now set \(\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1 \cup \mathcal{F}_2 \cup \cdots \cup \mathcal{F}_n\). Using (8)–(11) we have

\[
\partial \mathcal{F} = \bigcup_{i=0}^{n} (D_i \cup U_i).
\]
Rewrite $Z_k$ as $Z_k = \bigoplus_{i=1}^{n} Z_{q_i}$ and let us call weight of an element $x \in Z_k$ the number of nonzero coordinates of $x$. Note that $D_0$ is the set of zero divisors of weight 1, that $D_1 \cup D_n$ is the set of zero divisors of weight at least 2 and with nonzero $n$th coordinate, and finally that $D_i$, for $2 \leq i \leq n-1$, is the set of zero divisors of weight at least 2 and whose last nonzero coordinate is the $i$th one. This allows to recognize that the $D_i$’s partition $D(Z_k)$.

Then, recalling that the $U_i$’s are pairwise disjoint, we may conclude that $\partial F$ has no repeated elements and that all elements of $Z_k^* - \partial F$ are units.

Let $W = \{ \pm w_1, \ldots, \pm w_t \}$ be the complement of $\partial F$ in $Z_k^*$. Each $w_i$ is a unit in $Z_k$ so that $W_i = (0, w_i, 2w_i, \ldots, (k-1)w_i)$ is a Hamiltonian $k$-cycle of cotype 1. Obviously, we have $\partial W_i = \{ w_i, -w_i \}$ so that $\partial \{ W_1, \ldots, W_t \} = W$. It follows, by Proposition 1.5, that $\mathcal{F} \cup \{ W_1, \ldots, W_t \}$ is the set of base cycles of a cyclic Hamiltonian $k$-cycle system.

4. Cyclic $(K_{2kn+k}, C_k)$-designs

The existence question for $(K_v, C_k)$-designs has been completely settled by Alspach and Gavlas [1] in the case of $k$ odd (see also [5]) and by Šajna [16] in the even case.

Regarding cyclic $(K_v, C_k)$-designs, existence has been proved whenever $v \equiv 1 \pmod{2k}$. This, for $k$ even, was proved in the 1960s by Kotzig [9] and by Rosa [13,15] who also settled the case of $k = 3, 5, 7$ [14] (for the earliest solution of $k = 3$ see [11]). The case of $k$ odd > 7 was recently solved by the present authors [6]. Other existence solutions were independently found by Fu and Wu [7] and by Bryant et al. [2].

The main result of the present paper allows to give an almost complete solution to the existence problem for $(K_v, C_k)$-designs with $v \equiv k \pmod{2k}$. In fact, in [6] we have also proved the existence of a cyclic $(K_{m \times k}, C_k)$-design for any pair of odd integers $(m, k) \neq (3, 3)$. This, as observed in that paper, implies the existence of a cyclic $(K_v, C_k)$-design with $v \equiv k \pmod{2k}$ whenever a cyclic Hamiltonian $k$-cycle system exists. Hence we may state:

**Theorem 4.1.** If $k$ is an odd integer but $k \neq 15$ and $p^x$ with $p$ a prime and $x > 1$, then there exists a cyclic $(K_{2kn+k}, C_k)$-design for any non-negative integer $n$ but $(k,n) \neq (3,1)$.

We feel that for $n > 0$ the possible exceptions $k = 15$ and $k = p^x$ with $p$ a prime and $x > 1$ may be removed. For instance, the 9-cycles

$$A = (0, 1, 26, 3, 22, 4, 21, 8, 20),$$

$$B = (0, 3, 25, 9, 12, 7, 18, 21, 16),$$

$$C = (0, 6, 12, 18, 24, 3, 9, 15, 21),$$

are the base cycles of a cyclic $(K_9, C_9)$-design.
Acknowledgements

The authors wish to thank the anonymous referees for their useful comments which made this article more readable.

Note added in proof

When this paper was in press, the last open cases about the existence problem for cyclic \((k_{2n+k}, c_k)\)-designs have been settled in [17].

References

[17] A. Vietri, Cyclic \(k\)-cycle systems of order \(2kn + k\): a solution of the last open cases, preprint.