EXTENDING POTOČNIK AND ŠAJNA’S CONDITIONS ON THE EXISTENCE OF VERTEX-TRANSITIVE SELF-COMPLEMENTARY $k$-HYPERGRAPHS

LINDA LESNIAK

Western Michigan University, Kalamazoo, MI USA
e-mail: linda.lesniak@wmich.edu

HENRI THUILLIER

Université d’Orléans, France
e-mail: henri.thuillier@orange.fr

AND

A. PAWEL WOJDA

AGH University of Science and Technology, Kraków, Poland
e-mail: wojda@agh.edu.pl

Abstract

Let $\ell$ be a positive integer, $k = 2^\ell$ or $k = 2^\ell + 1$, and let $n$ be a positive integer with $n \equiv 1 \pmod{2^{\ell+1}}$. For a prime $p$, $n_{(p)}$ denotes the largest integer $i$ such that $p^i$ divides $n$. Potočnik and Šajna showed that if there exists a vertex-transitive self-complementary $k$-hypergraph of order $n$, then for every prime $p$ we have $p^{n_{(p)}} \equiv 1 \pmod{2^{\ell+1}}$. Here we extend their result to a larger class of integers $k$.

Keywords: vertex-transitive hypergraphs, self-complementary hypergraphs.

2010 Mathematics Subject Classification: 05C65.

1. Introduction

For a prime $p$ and a positive integer $n$, let $n(p)$ denote the largest integer $i$ for which $p^i$ divides $n$. Using this notation, we combine the theorems of Rao and Muzychuk as follows.

**Theorem 1.1** (Rao/Muzychuk). For a positive integer $n$, there exists a vertex-transitive self-complementary graph of order $n$ if and only if $p^{n(p)} \equiv 1 \pmod{4}$ for every prime $p$.

For an interesting discussion of the history of the vertex-transitive self-complementary graph problem, see [1].

For every integer $k \geq 2$, a $k$-uniform hypergraph, or $k$-hypergraph, for short, is a pair $(V; E)$ consisting of a vertex set $V$ and edge set $E \subseteq \binom{V}{k}$, where $\binom{V}{k}$ denotes the set of all $k$-subsets of $V$. Clearly a 2-hypergraph is just a simple graph. A hypergraph $H$ is called vertex-transitive if for every two vertices $u, v$ of $H$ there is an automorphism $\phi$ of $H$ for which $u = \phi(v)$. A $k$-hypergraph $H = (V; E)$ is called self-complementary if there is a permutation $\sigma$ of the set $V$, called a self-complementing permutation, such that for every $k$-subset $e$ of $V$, $e \in E$ if and only if $\sigma(e) \notin E$. In other words, $H$ is isomorphic to $\overline{H} = (V; \binom{V}{k} \setminus E)$. In 2009, Potočnik and Šajna [5] proposed studying the problem analogous to the previous theorem for $k$-hypergraphs. In particular, they extended Muzychuk’s necessary condition to $k$-hypergraphs when $k = 2^\ell$ or $k = 2^\ell + 1$ for some positive integer $\ell$. Shortly after, Gosselin [3] established the sufficiency of the Potočnik and Šajna result.

**Theorem 1.2** (Potočnik-Šajna/Gosselin). Let $m$ be a positive integer, $k = 2^m$ or $k = 2^m + 1$, and let $n$ be a positive integer with $n \equiv 1 \pmod{2^{m+1}}$. Then there exists a vertex-transitive self-complementary $k$-hypergraph of order $n$ if and only if for every prime $p$ we have $p^{n(p)} \equiv 1 \pmod{2^{m+1}}$.

In Theorem 1.2, the only considered values of $k$ are of the form $k = 2^m$ or $k = 2^m + 1$, for some positive integer $m$. We now consider any integer $k \geq 2$ and look at the binary expansion of $k$. Then there are positive integers $\ell$ and $m$ such that $k = \sum_{\ell \leq j < m} k_j 2^j + 2^m$ or $k = 1 + \sum_{\ell \leq j < m} k_j 2^j + 2^m$, where $k_i \in \{0, 1\}$, for every $i$. In Theorem 1.2, each such $k_\ell = 0$. Furthermore, in Theorem 1.2, $n \equiv 1 \pmod{2^{m+1}}$. This suggests our next theorem which extends the necessary condition of Potočnik and Šajna for more values of $k$.

**Theorem 1.3.** Let $\ell, k, n$ and $m$ be positive integers such that $1 < k < n$, $1 \leq \ell \leq m$ and $n \equiv 1 \pmod{2^{m+1}}$, $k = \sum_{\ell \leq j \leq m} k_j 2^j$ or $k = \sum_{\ell \leq j \leq m} k_j 2^j + 1$, where $k_j \in \{0, 1\}$ for every $j$, $\ell \leq j \leq m$. If there exists a vertex-transitive self-complementary $k$-hypergraph of order $n$, then for every prime $p$ we have $p^{n(p)} \equiv 1 \pmod{2^{\ell+1}}$. 
2. Proof of Theorem 1.3

If $H$ is a self-complementary $k$-hypergraph, then the set of all self-complementing permutations of $H$ will be denoted by $C(H)$. In [7] the following characterization of self-complementing permutations for $k$-hypergraphs was given. Here $|c|$ denotes the order of a cycle $c$.

**Theorem 2.1.** Let $n$ and $k$ be positive integers, $2 \leq k \leq n$. A permutation $\sigma$ of $[1, n]$ with cycles $c_1, \ldots, c_\lambda$ is a self-complementing permutation of a $k$-hypergraph of order $n$ if and only if there is a nonnegative integer $t$ such that the following hold.

(i) $k = a_t 2^\ell + s_t$, for some integers $a_t$ and $s_t$, where $a_t$ is odd and $0 \leq s_t < 2^\ell$;
(ii) $n = b_t 2^{\ell+1} + r_t$, for some integers $b_t$ and $r_t$, where $0 \leq r_t < 2^\ell + s_t$; and
(iii) $\sum_{\ell \leq |c_i| \leq t} |c_i| = r_t$.

In [7], the condition (iii) has the form of inequality $\sum_{\ell \leq |c_i| \leq t} |c_i| \leq r_t$. However, since $r_t = \sum_{\ell \leq |c_i| \leq t} |c_i| \mod 2^{\ell+1}$ and $r_t < 2^{\ell+1}$, we have equality (iii).

**Corollary 2.2.** Let $\ell, k, n$ and $m$ be positive integers such that $1 < k < n$, $1 \leq \ell \leq m$ and $n \equiv 1 \mod 2^{m+1}$, $k = \sum_{\ell \leq j \leq m} k_j 2^j$ or $k = \sum_{\ell \leq j \leq m} k_j 2^j + 1$, where $k_j \in \{0, 1\}$ for every $j$, $\ell \leq j \leq m$. Then every cycle of order greater than one of any self-complementing permutation of a self-complementary $k$-hypergraph of order $n$ has order divisible by $2^{\ell+1}$.

Note that any such a permutation has exactly one cycle of order one.

**Proof.** Let $\sigma$ be a self-complementing permutation of a self-complementary $k$-hypergraph of order $n$ with cycles $c_1, \ldots, c_\lambda$. By Theorem 2.1 there exists a nonnegative integer $t$ such that

1. $k = a_t 2^\ell + s_t$, where $a_t$ is odd and $0 \leq s_t < 2^\ell$,
2. $n = b_t 2^{\ell+1} + r_t$, $r_t \in \{0, \ldots, 2^\ell - 1 + s_t\}$, and
3. $\sum_{\ell \leq |c_i| \leq t} |c_i| = r_t$.

First observe that $t = 0$ implies $s_t = 0$, and hence $r_t = 0$ and $n$ is even, a contradiction. Thus, $t \geq 1$. Since $a_t$ is odd, it follows that $t \geq \ell$, and since $k < 2^{n+1}$, we have $t \leq m$. Consequently, as $n \equiv 1 \mod 2^{m+1}$, we have that $n \equiv 1 \mod 2^{\ell+1}$ and $r_t = 1$. Thus, exactly one cycle $c_1$, necessarily of length 1, satisfies (3). In other words, with exception of a single fixed point, every cycle of $\sigma$ has order divisible by $2^{\ell+1}$, and hence by $2^{\ell+1}$. □

The proof of Theorem 1.3 uses the technique of Muzychuk [2]. The proof also depends on the first two Sylow theorems (see [4], for example). The following theorem is well-known. We give it however with proof, for completeness.
Theorem 2.3. Let $p$ be a prime and $G$ a finite group. If $P$ is a Sylow $p$-subgroup of its normalizer in $G$, then $P$ is a Sylow $p$-subgroup of the group $G$.

Proof. To prove this theorem, we shall use the notion of group action. If we have a group $G$ acting on a set $X$, we use symbols $X_{fix}$, $G_x$, and $O_x$ to denote the set of all fixed points of $X$, the stabilizer of a point $x$ in $G$, and the orbit of $x$, respectively. Recall that for any point $x$, the Orbit-Stabilizer Theorem (see, for instance, [4] Section 8.3 Lemma 3) asserts that $|O_x| = |G/G_x|$, and clearly $O_x = \{x\}$ if and only if $G_x = G$.

The well-known Orbit Decomposition Theorem (see [4]) states that if a group $G$ acts on a finite set $X \neq \emptyset$, and $x_1, \ldots, x_n \in X$ are representatives of mutually disjoint orbits with at least two elements, then

$$|X| = |X_{fix}| + \sum_{i=1}^{n} |G/G_{x_i}|.$$ 

Thus, the Orbit Decomposition Theorem implies that if $G$ is a $p$-group, then

$$|X| \equiv |X_{fix}| \pmod{p}.$$ 

By $N_G(H)$ we denote the normalizer of a subgroup $H$ in $G$; that is the largest subgroup of $G$ in which $H$ is normal, namely $N_G(H) = \{g \in G : gHg^{-1} = H\}$. Now we have the following fact.

Fact. If $H$ is a $p$-subgroup of $G$, then $|N_G(H)/H| \equiv |G/H| \pmod{p}$.

To prove it, we consider the following action of $H$ on the set $G/H$ of right cosets: for every $a \in H$ and every coset $Hb$, we define $a(Hb) = Hba^{-1}$. It is straightforward to verify that we are indeed defining a group action. Clearly, for every $a \in H$, and for every $b \in G$, $Hba^{-1} = Hb$ if and only if $bab^{-1} \in H$, and hence, $(G/H)_{fix} = N_G(H)/H$. Since $H$ is a $p$-group, $|G/H| - |N_G(H)/H| = |G/H| - |(G/H)_{fix}|$ is divisible by $p$. If $P$ is a Sylow $p$-subgroup of $N_G(P)$, then $|N_G(P)/P| \not\equiv 0 \pmod{p}$, and by our Fact, it follows that $P$ is a Sylow $p$-subgroup of $G$.

Proof of Theorem 1.3.

Suppose that $H = (V; E)$ is a self-complementary vertex-transitive $k$-hypergraph of order $n$, where $k$ and $n$ satisfy the conditions of our theorem. Let $p$ be a prime; if $n(p) = 0$, then the result is clear. Thus assume that $n(p) > 0$. We shall find a self-complementary vertex-transitive $k$-subhypergraph $H'$ of $H$ of order $p^{n(p)}$ such that the cycles of a self-complementing permutation of $H'$ are cycles of a self-complementing permutation $\sigma$ of $H$ and the fixed point of $\sigma$ is one of the vertices of $H'$. By Corollary 2.2, all cycles of $\sigma$ have order divisible by $2^{\ell+1}$,
with the exception of a single fixed point. Hence the order of \(H^t\), that is \(p^{r(n)}\), is congruent to 1 modulo \(2^{l+1}\), and the statement of Theorem 1.3 follows.

Let \(M = \text{Aut}(H)\) be the automorphism group of \(H\). For any group \(K\), denote the set of the Sylow \(p\)-subgroups of \(K\) by \(\text{Syl}_p(K)\).

Note that for every \(\sigma \in C(H)\) we have \(\sigma^2 \in \text{Aut}(H)\). Moreover a product of a number of automorphisms and self-complementing permutations is an automorphism of \(H\) if the number of self-complementing permutations is even; otherwise, the product is a self-complementing permutation of \(H\). The set \(G = \text{Aut}(H) \cup C(H)\) is a group which is generated by \(\text{Aut}(H) \cup \{\sigma\}\), where \(\sigma\) is an arbitrary element of \(C(H)\).

Define \(P\) to be the set of \(p\)-subgroups \(P\) of \(M\) with the property that there exists a vertex \(v\) of \(H\) and \(\tau \in C(H)\) such that

1. \(\tau(v) = v;\)
2. \(\tau P\tau^{-1} = P\) (\(\tau\) normalizes \(P\));
3. \(P_v \in \text{Syl}_p(M_v)\).

We will show that \(P\) is not empty and any maximal element of \(P\) is, in fact, a Sylow \(p\)-subgroup of \(M\).

Since \(H\) is self-complementary, \(C(H)\) is not empty. Choose any \(\sigma \in C(H)\).

By Corollary 2.2 there is a fixed point \(v\) of \(\sigma\). Let \(P \in \text{Syl}_p(M_v)\).

Note that if \(p\) does not divide \(|M_v|\), then \(P\) is trivial. Since \(P\) is a subgroup of \(M_v\), then \(P = P_v\), and clearly \(\sigma P \sigma^{-1}\) is a subgroup of \(M_v\) isomorphic to \(P\).

By the second Sylow Theorem, there exists \(g \in M_v\) such that \(\sigma P \sigma^{-1} = gPg^{-1}\).

Set \(\tau = g^{-1}\sigma\). Then \(\tau \in C(H)\), \(\tau(v) = v\), \(\tau P\tau^{-1} = P\), and \(P_v \in \text{Syl}_p(M_v)\). Hence \(P \in P\) and \(P \neq \emptyset\).

From now on we shall assume that

- \(P \in P\) is a maximal element of \(P\),
- \(N\) is the normalizer of \(P\) in \(M\),
- \(Q\) is a Sylow \(p\)-subgroup of \(N\) containing \(P\) (\(Q\) exists by the second Sylow Theorem).

Claim. \(P\) is a Sylow \(p\)-subgroup of \(M\).

Proof. To prove this claim, it suffices to show that \(Q \in P\), and hence \(Q = P\) by the maximality of \(P\). It will then follow that \(P\) is a Sylow \(p\)-subgroup of its own normalizer in \(M\), and hence by Theorem 2.3, it is a Sylow \(p\)-subgroup of \(M\).

Since \(P \in P\), there are \(\tau \in C(H)\) and a vertex \(v\) such that \(\tau(v) = v\), \(\tau P\tau^{-1} = P\) and \(P_v \in \text{Syl}_p(M_v)\). It is straightforward to show that \(\tau\) normalizes \(N\), that is, \(\tau N\tau^{-1} = N\). Thus, \(\tau N = N\tau\).

Since \(Q\) is a subgroup of \(N\) and \(\tau N\tau^{-1} = N\), we have that \(\tau Q\tau^{-1}\) is a subgroup of \(N\) and since \(|\tau Q\tau^{-1}| = |Q|\), we conclude that \(\tau Q\tau^{-1}\) is a Sylow \(p\)-subgroup of \(N\).
Recall that $v$ is a fixed point of $\tau$, and let $U = N(v)$, where $N(v) = \{h(v): h \in N\}$. Then we have $\tau(U) = \tau(N(v)) = (\tau N)(v) = (N\tau)(v)$, since $\tau N = N\tau$ by our previous argument. This implies that $\tau(U) = N(\tau(v)) = N(v) = U$.

By Corollary 2.2, every cycle $c$ of the self-complementing permutation $\tau$ has length divisible by $2^{\ell+1}$, with the exception of one fixed point. Since $\tau(U) = U$, for every cycle $c$ of the permutation $\tau$ we know that either all the vertices of $c$ are in $U$ or else, the set of vertices of $c$ is disjoint with $U$. Therefore, $U$ is a set of vertices of a self-complementary vertex-transitive $k$-hypergraph $H' = (U; E \cap \binom{U}{k})$ with self-complementing permutation $\tau$ (restricted to $U$) and vertex-transitive group of automorphisms containing $N$. Moreover, vertex $v$, the fixed point of $\tau$, is in $U$. Hence we have

$$|U| \equiv 1 \pmod{2^{\ell+1}}.$$ 

Since $\tau Q \tau^{-1}$ and $Q$ are two Sylow $p$-subgroups of the group $N$, by the second Sylow Theorem, there is $g \in N$ such that $\tau Q \tau^{-1} = g Q g^{-1}$.

Hence $(g^{-1} \tau) Q (g^{-1} \tau)^{-1} = Q$.

Write $\sigma = \tau^{-1} g$. By the definition of $U$ and since $g \in N$, we have $g(U) = U$, and hence, $\sigma(U) = U$. We have $\sigma Q \sigma^{-1} = Q$, and the restriction of $\sigma \in C(H)$ to the set $U$ is also a self-complementing permutation of $H'$.

By Corollary 2.2, the permutation $\sigma$ has a fixed point $u$, and all remaining cycles are of lengths congruent to $1 \pmod{2^{\ell+1}}$. Since $|U| \equiv 1 \pmod{2^{\ell+1}}$ and the cycles of the restriction of $\sigma$ to $U$ are the cycles of $\sigma$, we have $u \in U$.

Since the group $N$ is transitive on the set $U$, there is $h \in N$ such that $h(v) = u$. Thus the subgroups $M_u$ and $M_u$ are conjugate, that is,

- $M_u = h M_v h^{-1}$.

Moreover, we also have

- $P_u = P_v h^{-1}$.

Hence $|M_u| = |M_u|$ and $|P_u| = |P_u|$, and therefore $P_u$ is a Sylow $p$-subgroup of $M_u$. Since $P_u \leq Q_u \leq M_u$ and $Q_u$ is a $p$-subgroup of $M_u$, it follows that $Q_u = P_u$ and $Q_u$ is a Sylow $p$-subgroup of $M_u$. Finally, we have $Q \in \mathcal{P}$. This completes the proof of the claim.

Now we shall show that the orbit $P(v)$ induces a self-complementary vertex-transitive $k$-hypergraph of order $p^r$, where $r = n(p)$. Note first that since $\tau P = P\tau$ and $\tau(v) = v$, we have

$$\tau(P(v)) = P(\tau(v)) = P(v)$$

and therefore the $k$-subhypergraph of $H$ induced by $P(v)$ is self-complementary and vertex-transitive.
Write $|M| = p^d q$, where $q$ and $p$ are relatively prime. Then $|P| = p^d$ by the Claim. Since $M$ acts transitively on $V$ we have

$$|M_v| = \frac{|M|}{|M(v)|} = \frac{p^d q}{p^r m} = p^{d-r} s,$$

for some positive integers $m$ and $s$ both relatively prime with $p$.

Since $P_v \in \text{Syl}_p(M_v)$, it follows that $|P_v| = p^{d-r}$. On the other hand, since $P \in \text{Syl}_p(M)$ and $P_v \in \text{Syl}_p(M_v)$ we have

$$p^{d-r} = |P_v| = \frac{|P|}{|P(v)|} = \frac{p^d}{|P(v)|}.$$ 

This implies $|P(v)| = p^r$. Since $\tau$ is a self-complementing permutation of $H$, by Corollary 2.2, the length of every cycle of $\tau$, with exception of a single fixed point, is divisible by $2^\ell + 1$. Since $\tau(P(v)) = P(v)$, we know that $P(v)$ is the union of orbits of $\tau$, including the fixed point $v$. Hence $p^r \equiv 1 \pmod{2^\ell + 1}$ as claimed.

Acknowledgement

The authors express their thanks to the anonymous referees for reading carefully the manuscript and for their important comments.

References


