Vertex-transitive q-complementary uniform hypergraphs

Shonda Gosselin[*]

Department of Mathematics and Statistics, University of Winnipeg
515 Portage Avenue, Winnipeg, MB R3B 2E9, Canada

s.gosselin@uwinnipeg.ca

Abstract

For a positive integer q, a k-uniform hypergraph $X = (V, E)$ is q-*complementary* if there exists a permutation θ on V such that the sets $E, E^\theta, E^{\theta^2}, \ldots, E^{\theta^{q-1}}$ partition the set of k-subsets of V. The permutation θ is called a q-*antimorphism* of X. The well studied self-complementary uniform hypergraphs are 2-complementary.

For an integer n and a prime p, let $n_{(p)} = \max\{i : p^i \text{ divides } n\}$. In this paper, we prove that a vertex-transitive q-complementary k-hypergraph of order n exists if and only if $n^{n_{(p)}} \equiv 1 \pmod{q^{\ell+1}}$ for every prime number p, in the case where q is prime, $k = bq^\ell$ or $k = bq^\ell + 1$ for a positive integer $b < k$, and $n \equiv 1 \pmod{q^{\ell+1}}$. We also find necessary conditions on the order of these structures when they are t-fold-transitive and $n \equiv t \pmod{q^{\ell+1}}$, for $1 \leq t < k$, in which case they correspond to large sets of isomorphic t-designs. Finally, we use group theoretic results due to Burnside and Zassenhaus to determine the complete group of automorphisms and q-antimorphisms of these hypergraphs in the case where they have prime order, and then use this information to write an algorithm to generate all of these objects. This work extends previous, analagous results for vertex-transitive self-complementary uniform hypergraphs due to Muzychuk, Potočnik, Šajna, and the author. These results also extend the previous work of Li and Praeger on decomposing the orbitals of a transitive permutation group.

Key words: Self-complementary hypergraph; t-complementary hypergraph; Uniform hypergraph; Transitive hypergraph; Complementing permutation; Large set of t-designs

---

1 Introduction

1.1 Definitions and notation

For a finite set V and a positive integer k, let $V^{(k)}$ denote the set of all k-subsets of V. A *hypergraph* with vertex set V and edge set E is a pair (V, E), in which V is a finite set and E is a collection of subsets of V. A hypergraph (V, E) is called *k-uniform* (or a *k-hypergraph*) if E is a subset of $V^{(k)}$. The parameters k and $|V|$ are called the *rank* and the *order* of the k-hypergraph, respectively. The vertex set and the edge set of a hypergraph X will often be denoted by $V(X)$ and $E(X)$, respectively. A 2-hypergraph is a *graph*.

An *isomorphism* between k-hypergraphs X and X' is a bijection $\phi : V(X) \to V(X')$ which induces a bijection from $E(X)$ to $E(X')$. If such an isomorphism exists the hypergraphs X and X' are said to be *isomorphic*. An *automorphism* of X is an isomorphism from X to X. The set of all automorphisms of X will be denoted by $Aut(X)$. Clearly, $Aut(X)$ is a subgroup of $Sym(V(X))$, the symmetric group of permutations on $V(X)$.

For a positive integer q, a k-hypergraph $X = (V, E)$ is *cyclically q-complementary* (or *q-complementary*) if there exists a permutation θ on V such that the sets $E, E^\theta, E^{\theta^2}, \ldots, E^{\theta^{q-1}}$ partition $V^{(k)}$. We denote the set E^{θ^i} by E_i. Note that $E_i^\theta = E_{i+1}$ for $i = 0, 1, \ldots, t-2$ and $E_{q-1}^\theta = E_0 = E$. Such a permutation θ is called a *(q,k)-complementing permutation*, and it gives rise to a family of q isomorphic k-hypergraphs $\{X_i = (V, E_i) : i = 0, 1, \ldots, q-1\}$ which partition $V^{(k)}$, the complete k-hypergraph on V, and which are permuted cyclically under the action of θ. The following facts in [2] about (q, k)-complementing permutations follow from the definition.

Lemma 1.1. [2] *Let V be a finite set, and let s, q and k be positive integers such that $\gcd(q, s) = 1$.*

(1) *A permutation $\theta \in Sym(V)$ is a (q, k)-complementing permutation if and only if θ^s is a (q, k)-complementing permutation.*

(2) *The order of a (q, k)-complementing permutation is divisible by q.*

(3) *If q is prime, every cyclically q-complementary k-hypergraph has a (q, k)-complementing permutation with order a power of q.*

A (q, k)-complementing permutation of a q-complementary k-hypergraph X is also called a *q-antimorphism* of X, and the set of q-antimorphisms of X will be denoted by $Ant_q(X)$. It is not difficult to check that $Aut(X) \cup Ant_q(X)$ is a subgroup of $Sym(V)$, and that $Aut(X)$ is an index-q subgroup of $Aut(X) \cup Ant_q(X)$. Also, if $\theta \in Ant_q(X)$ then $\theta^{qs} \in Aut(X)$ for all integers s. Finally, it is clear that $Aut(X) = Aut(X_i)$ for $i = 0, 1, \ldots, q-1$ when X is q-complementary.

Let $X = (V, E)$ be a k-hypergraph, let t be a positive integer, $t < k$. A k-hypergraph X is called *t-subset-regular* if there is a constant c such that every t-subset of V is contained in exactly c edges in E. A k-hypergraph X is called *vertex-transitive* (or

simple *transitive*) if $Aut(X)$ acts transitively on $V(X)$, and it is called *t-fold-transitive* (or *t-transitive*) if $Aut(X)$ acts transitively on the set of ordered t-tuples of distinct vertices of X. The 2-transitive hypergraphs are also called *doubly-transitive*. Clearly, every t-transitive k-hypergraph is t-subset-regular.

If Ω is a finite set, v is a point in Ω, τ is a permutation on Ω, G is a permutation group on Ω, and p is a prime, then v^τ, v^G, G_v, and $Syl_p(G)$ will denote the image of v by τ, the orbit of G containing v, the stabilizer of the point v in the group G, and the set of Sylow p-subgroups of G, respectively. For a prime power n, let $\mathbb{F}_n^*$ denote the (cyclic) multiplicative group of units of the finite field $\mathbb{F}_n$ of order n. Given $a \in \mathbb{F}_n^*$ and $b \in \mathbb{F}_n$, let $\alpha_{a,b}$ denote the permutation in $Sym(\mathbb{F}_n)$ defined by $\alpha_{a,b} : x \to ax + b$. The set $\{\alpha_{a,b} : a \in \mathbb{F}_n^*, \ b \in \mathbb{F}_n\}$ forms a group, called the *affine linear group of permutations* acting on $\mathbb{F}_n$. This group will be denoted by $AGL_1(n)$. For finite sets U and V, and any permutation $\alpha \in Sym(U)$ and $\beta \in Sym(V)$, the permutation $(\alpha, \beta) \in Sym(U \times V)$ is defined by $(u, v)^{(\alpha,\beta)} = (u^\alpha, v^\beta)$, for all $(u, v) \in U \times V$. If a H is a subgroup of a group G, we will denote this by $H \leq G$. If H and G are equivalent as permutation groups, we will denote this by $H \equiv G$.

A permutation group G acting on a finite set Ω is *sharply transitive* if for any two points $\alpha, \beta \in \Omega$, there is exactly one permutation $g \in G$ which maps α to β. The group G is *sharply doubly-transitive* if G is sharply transitive in its action on ordered pairs of distinct elements from Ω.

1.2 History and statement of the main results

The following result is actually a corollary to a more general result due to Khosrovshahi and Tayfeh-Rezaie in [5], which gives necessary conditions on the order of large sets of t-designs.

Lemma 1.2. [5] *Let q be prime and suppose that k or $k-1$ is equal to bq^ℓ, where $1 \leq b \leq q-1$ for some positive integer ℓ. Let t be a positive integer such that $1 \leq t < k$. If there exists a t-subset regular q-complementary k-hypergraph of order n, then $n \equiv j \ (\mathrm{mod} \ q^{\ell+1})$ for some $j \in \{t, t+1, \ldots, k-1\}$.*

As vertex-transitive q-complementary k-hypergraphs are necessarily 1-subset-regular, we can use Lemma 1.2 to find basic necessary conditions on their order n in the case where k or $k-1$ is equal to bq^ℓ for a positive integer $b < q$. In particular, $n \equiv j \ (\mathrm{mod} \ q^{\ell+1})$ for some $j \in \{1, 2, \ldots, k-1\}$. However, the main result of this paper in Theorem 1.3 shows that the condition of transitivity implies much stronger necessary conditions on the order of these structures in the case where $n \equiv 1 \ (\mathrm{mod} \ q^{\ell+1})$, and that these necessary conditions are also sufficient.

We will make use of the following notation. For a positive integer n and a prime p, let $n_{(p)}$ denote the greatest integer r such that p^r divides n.

Theorem 1.3. *Let q be prime, let ℓ and b be positive integers such that $1 \leq b \leq q-1$, and suppose that k or $k-1$ equals bq^ℓ. If $n \equiv 1 \ (\mathrm{mod} \ q^{\ell+1})$, then there exists a vertex-*

transitive q-complementary k-hypergraph of order n if and only if

$$p^{n_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \textit{for every prime } p. \tag{1}$$

The necessity of condition (1) has been proved previously in the case where $q = 2$ by Potočnik and Šajna [12], and their proof technique is used in Section 2 in the proof of the necessity of this condition in the general case where q is prime. It has also been shown previously that condition (1) is sufficient in the case where $q = 2$ [3]. In Section 3, we present a construction for vertex-transitive q-complementary uniform hypergraphs to prove that this condition is also sufficient for every odd prime q, which will complete the proof of Theorem 1.3.

Now consider hypergraphs with a greater level of symmetry, namely those which are t-fold-transitive for $t > 1$. Since t-fold-transitive q-complementary k-hypergraphs are t-subset-regular, Lemma 1.2 gives basic necessary conditions on their order n in the case where k or $k-1$ is equal to bq^ℓ for an integer b such that $1 \le b \le q-1$. In particular, $n \equiv j \pmod{q^{\ell+1}}$ for some $j \in \{t, t+1, \ldots, k-1\}$. However, in Section 2 we will extend the necessary conditions of Theorem 1.3 to obtain the following theorem, which gives stronger necessary conditions on the order n of such a hypergraph in the case where $n \equiv t \pmod{q^{\ell+1}}$.

Theorem 1.4. *Let ℓ be a positive integer, let q be prime, and suppose that k or $k-1$ is equal to bq^ℓ for a positive integer $b < q$. Let t be a positive integer, $t < k$, and let $n \equiv t \pmod{q^{\ell+1}}$. If there exists a t-fold-transitive q-complementary k-hypergraph of order n, then*

$$p^{(n-t+1)_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \textit{for every prime } p. \tag{2}$$

In Section 4, we will use group theoretic results due to Burnside and Zassenhaus to determine the group of automorphisms and q-antimorphisms of a vertex-transitive q-complementary k-hypergraph of prime order under certain conditions on p, q and k, and then we will use this information to obtain Algorithm 4.6 for generating all such hypergraphs.

1.3 Connection to design theory

There is a connection between t-subset-regular hypergraphs and designs. If a t-subset regular k-hypergraph X of order n is q-complementary, then each of the hypergraphs $X_0, X_1, \ldots, X_{q-1}$ is a t-(n, k, λ) *design*, as defined in [1], with $\lambda = \binom{n-t}{k-t}/q$, and the set $\{X_0, X_1, \ldots, X_{q-1}\}$ is a *large set of t-designs* [1], denoted by $LS[q](t, k, n)$, in which the t-designs are isomorphic. If X is vertex-transitive, then the corresponding t-design is point-transitive. Hence vertex-transitive q-complementary k-hypergraphs of order n correspond bijectively to large sets of t-designs $LS[q](t, k, n)$ for some $t \ge 1$ in which the t-designs are point-transitive and isomorphic. Large sets of t-designs are very important structures in combinatorial design theory, and their construction forms a crucial part of Teirlinck's remarkable proof in [15] of the existence of t-designs for all t. Large sets of t-designs also have useful applications in cryptography, which is essential to the security

of communication networks and, consequently, they have been studied extensively. The results to date have been compiled efficiently in [1, pp.98-101]. Some sufficient conditions on the order of large sets in which the t-designs have a common automorphism group have been obtained but, to date, few large sets of isomorphic t-designs have been constructed. The results of this paper imply the corresponding results in design theory. In particular, Theorem 1.3 and Theorem 1.4 imply the following two results, respectively.

Corollary 1.5. *Let q be prime, let ℓ and b be positive integers such that $1 \leq b \leq q - 1$, and suppose that k or $k - 1$ equals bq^ℓ and $n \equiv 1 \pmod{q^{\ell+1}}$. If*

$$p^{n_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \text{for every prime } p, \tag{3}$$

then there exists a $LS[q](1, k, n)$ in which the 1-designs are point-transitive and isomorphic. Moreover, if the designs in a $LS[q](1, k, n)$ are point-transitive and permuted cyclically by a permutation θ of the point set, then condition (3) is also necessary.

Corollary 1.6. *Let ℓ be a positive integer, let q be prime, and suppose that k or $k - 1$ is equal to bq^ℓ for a positive integer $b < q$. Let t be a positive integer, $t < k$, and let $n \equiv t \pmod{q^{\ell+1}}$. If there exists a $LS[q](t, k, n)$ in which the t-designs are t-fold-transitive and permuted cyclically by a permutation θ of the point set, then*

$$p^{(n-t+1)_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \text{for every prime } p.$$

In this paper, we will use terminology from hypergraph theory, rather than design theory.

2   Necessary conditions on order

In this section we prove the necessity of condition (1) in Theorem 1.3. First we state some preliminary results.

We will need to make use of the following lemma which is actually a corollary to a result in [2]. Lemma 2.1 characterizes the cycle type of the (q, k)-complementing permutations in $Sym(n)$ which have order equal to a power of q, in the case where q is prime, for certain values of k and n.

Lemma 2.1. [2] *Let q be prime, and suppose that k or $k - 1$ is equal to bq^ℓ for some integer b such that $1 \leq b \leq q - 1$. Let $n \equiv 1 \pmod{q^{\ell+1}}$, and let $\theta \in Sym(n)$ be a permutation whose order is a power of q. Then θ is a (q, k)-complementing permutation if and only if θ has exactly one fixed point and every nontrivial orbit of θ has length divisible by $q^{\ell+1}$.*

We will also require the following useful and well-known counting tool, called the *orbit-stabilizer* lemma.

Lemma 2.2. (Orbit-stabilizer [16]) *Let G be a permutation group acting on V and let x be a point in V. Then*

$$|G| = |G_x||x^G|.$$

We are now ready to state and prove the necessity of condition (1) of Theorem 1.3. The proof is essentially the same as Potočnik and Šajna's proof of this result in [12] for the case where $q = 2$, but it is included here for the sake of completeness. It should be noted that a restricted version of Theorem 2.3 for graphs ($k = 2$) follows from the work of Li and Praeger in [7]. Previously, Muzychuk proved this result in the case where $k = 2$ and $q = 2$ in [10].

Theorem 2.3. *Let q be prime, let ℓ and b be positive integers such that $1 \leq b \leq q - 1$, and suppose that k or $k - 1$ is equal to bq^ℓ. If $n \equiv 1 \pmod{q^{\ell+1}}$ and there exists a vertex-transitive q-complementary k-hypergraph of order n, then*

$$p^{n_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \text{for every prime } p.$$

Proof: Suppose that X is a vertex-transitive q-complementary k-hypergraph of order n. If a prime p does not divide n, then $n_{(p)} = 0$ and so the result holds, so we need only consider prime divisors of n. Let p be a prime divisor of n, and suppose that p^r is the highest power of p dividing n. We shall prove the theorem by finding a vertex-transitive q-complementary k-subhypergraph X' of X of order p^r, and the result will then follow from Lemma 1.2.

Let d be the largest positive integer such that p^d divides $|Aut(X)|$. The subhypergraph X' we are looking for will be induced by an appropriate orbit of a Sylow p-subgroup of $Aut(X)$. In the following four steps, we find an appropriate Sylow p-subgroup P of $Aut(X)$ and an orbit of P that induces a vertex-transitive q-complementary k-subhypergraph X' of order p^r.

Step 1. Define the set $\mathcal{P}$ of all p-subgroups P of $Aut(X)$ for which there exist $v \in V(X)$ and $\tau \in Ant_q(X)$ such that $v^\tau = v$, $\tau^{-1}P\tau = P$, and $P_v \in Syl_p(Aut(X)_v)$. We will show that $\mathcal{P} \neq \emptyset$, and that a maximal element of $\mathcal{P}$ is a Sylow p-subgroup of $Aut(X)$ with the desired properties.

Step 2. We show that $\mathcal{P} \neq \emptyset$. Choose $v \in V(X)$, $P \in Syl_p(Aut(X)_v)$, and $\sigma \in Ant_q(X)$. Since $Aut(X)$ is transitive on $V(X)$, there exists $h \in Aut(X)$ such that $v^h = v^\sigma$. Then $\bar{\sigma} := h\sigma^{-1}$ is a q-antimorphism of X fixing v. This implies that $\bar{\sigma}^{-1}Aut(X)_v\bar{\sigma} = Aut(X)_v$, and thus $\bar{\sigma}^{-1}P\bar{\sigma} \in Syl_p(Aut(X)_v)$. Therefore, there is $g \in Aut(X)_v$ such that $g^{-1}Pg = \bar{\sigma}^{-1}P\bar{\sigma}$. Let $\tau = g\bar{\sigma}^{-1}$. Then $v^\tau = v$ and $\tau^{-1}P\tau = P$. Moreover, $P_v = P \in Syl_p(Aut(X)_v)$. Hence $P \in \mathcal{P}$ and so $\mathcal{P} \neq \emptyset$.

Step 3. Let P be a maximal element of $\mathcal{P}$ with respect to inclusion. We show that P is a Sylow p-subgroup of $Aut(X)$. Let N be the normalizer of P in $Aut(X)$, and let Q be the Sylow p-subgroup of N containing P. We will show that Q lies in $\mathcal{P}$, and consequently $P = Q$ since P is a maximal element of $\mathcal{P}$ and $P \leq Q \in \mathcal{P}$. It will then follow that P is a Sylow p-subgroup of its own normalizer in $Aut(X)$, and therefore that P is a Sylow p-subgroup of $Aut(X)$.

Now we will show that $Q \in \mathcal{P}$. Since $P \in \mathcal{P}$, by the definition of $\mathcal{P}$, there exists $v \in V(X)$ and $\tau \in Ant_q(X)$ such that $v^\tau = v$, $\tau^{-1}P\tau = P$, and $P_v \in Syl_p(Aut(X)_v)$.

Since τ normalizes both $Aut(X)$ and P, it also normalizes N, and hence $\tau^{-1}Q\tau \in Syl_p(N)$. Let g be an element of N such that $\tau^{-1}Q\tau = g^{-1}Qg$. Then $g\tau^{-1} \in Ant_q(X)$, and so by Lemma 1.1(2), $|g\tau^{-1}| = sq^i$ for a positive integer i and an integer s such that $q \nmid s$. Now $\sigma = (g\tau^{-1})^s$ has order a power of q, and so by Lemma 2.1, σ fixes exactly one point of $V(X)$ and every other orbit of σ has order divisible by $q^{\ell+1}$. Let u be the unique fixed point of σ. Now we have a vertex u and a q-antimorphism σ such that $u^\sigma = u$, and $\sigma^{-1}Q\sigma = Q$, which are the first two requirements for Q to be in $\mathcal{P}$.

It remains to show that $Q_u \in Syl_p(Aut(X)_u)$. Let U be the orbit of N containing v. That is, $U = v^N$. Observe that $\tau^{-1}N\tau = N$, whence $U^\tau = v^{N\tau} = v^{\tau N} = v^N = U$. Since $g \in N$, we also have $U^g = U$. Hence $U^\sigma = U$. Thus the k-hypergraph with vertex set U and edge set $E(X) \cap U^{(k)}$ admits N as a transitive group of automorphisms and σ (restricted to U) as a q-antimorphism. Now by Lemma 1.2, it follows that its order $|U|$ is congruent to one of $1, 2, \ldots,$ or $k-1$ modulo $q^{\ell+1}$. Moreover, U is a union of orbits of σ, whose lengths (with the exception of the fixed point u) are all divisible by $q^{\ell+1}$. It follows that $|U| \equiv 1 (\mathrm{mod}\ q^{\ell+1})$ and the fixed point u of σ lies in U. Now since u and v lie in the same orbit of N, P_u and P_v are conjugate in N, and so $|P_u| = |P_v|$. It follows that $P_u \in Syl_p(Aut(X)_u)$. On the other hand, Q_u is a p-subgroup of $Aut(X)_u$ and $P_u \leq Q_u$, and so it follows that $Q_u = P_u$. Hence $Q_u \in Syl_p(Aut(X)_u)$, and we conclude that $Q \in \mathcal{P}$. It now follows that $P = Q$ and P is a Sylow p-subgroup of $Aut(X)$.

Step 4. Now we will show that the orbit of P containing v induces a k-hypergraph with the required properties. First, since $|P| = p^d$ and $P_v \in Syl_p(Aut(X)_v)$, we have $|P_v| = p^{d-r}$ and thus $|v^P| = p^r$ by the Orbit-Stabilizer Lemma 2.2. Second, since $(v^P)^\tau = (v^\tau)^P = v^P$, τ is a q-antimorphism of the k-hypergraph X' with vertex set v^P and edge set $E(X) \cap (v^P)^{(k)}$. Also $P \leq Aut(X)$, so P (restricted to v^P) is contained in $Aut(X')$. Since P certainly acts transitively on its orbit v^P, it follows that X' is a vertex-transitive q-complementary k-subhypergraph of X of order p^r, as required.

Now that Steps 1-4 are complete, it remains to show that the order p^r of X' is congruent to 1 modulo $q^{\ell+1}$. Observe that τ also lies in $Ant_q(X)$, and Lemma 1.1(2) guarantees that τ has order divisible by q. Thus $|\tau| = sq^i$ for positive integers i and s where $q \nmid s$, and so $\tau^s \in Ant_q(X)$ and τ^s has order a power of q. Hence Lemma 2.1 implies that τ^s has one fixed point, and every nontrivial orbit of τ^s has length divisible by $q^{\ell+1}$. By Lemma 1.2, $|V(X')| = |v^P|$ is congruent to one of $1, 2, \ldots,$ or $k-1$ modulo $q^{\ell+1}$. But since v^P is also a union of orbits of τ^s, we must have that $p^{n(p)} = p^r = |v^P| \equiv 1(\mathrm{mod}\ q^{\ell+1})$, as claimed. $\square$

Next we extend the necessary condition in Theorem 2.3 to prove Theorem 1.4.

Proof of Theorem 1.4: When $t = 1$ the result follows directly from Theorem 2.3, so we may assume that $t \geq 2$.

Suppose that $X = (V, E)$ is a t-transitive q-complementary k-hypergraph of order $n \equiv t \pmod{q^{\ell+1}}$. Let $v_1, v_2, \ldots, v_{t-1} \in V$, and let $\tau \in Ant_q(X)$. Since X is t-transitive, it is certainly $(t-1)$-transitive, and so there exists $\sigma \in Aut(X)$ such that $v_i^{\tau\sigma} = (v_i^\tau)^\sigma = v_i$

for all $i \in \{1, 2, \ldots, t-1\}$. Hence $\tau\sigma$ fixes $\{v_1, \ldots, v_{t-1}\}$ pointwise and $\tau\sigma \in Ant_q(X)$. That is, there exists a q-antimorphism $\theta = \tau\sigma$ of X which fixes every element in the set $\{v_1, \ldots, v_{t-1}\}$. Hence $E_0, E_1, E_2, \ldots, E_{q-1}$ partitions $V^{(k)}$, where $E_j = E^{\theta^j}$ for $j = 0, 1, \ldots, q-1$. Also, since X is t-transitive, it follows that $\bigcap_{i=1}^{t-1} Aut(X)_{v_i}$ acts transitively on $V \setminus \{v_1, v_2, \ldots, v_{t-1}\}$.

Let F denote the set of edges of E which do not contain an element of $\{v_1, v_2, \ldots, v_{t-1}\}$, and for each $j \in \{0, 1, 2, \ldots, q-1\}$, let F_j denote the edges in $E_j = E^{\theta^j}$ which do not contain an element of $\{v_1, v_2, \ldots, v_{t-1}\}$. Then every permutation in $\bigcap_{i=1}^{t-1} Aut(X)_{v_i}$ must map edges in F_j onto edges in F_j, and the permutation $\theta \in Ant_q(X)$ must map edges in F_j onto edges in $F_{j+1 \pmod q}$, for $j = 0, 1, \ldots, q-1$. Hence $F, F^\theta, F^{\theta^2}, \ldots, F^{\theta^{q-1}}$ partitions $(V \setminus \{v_1, v_2, \ldots, v_{t-1}\})^{(k)}$, and so θ is a q-antimorphism of the k-hypergraph $\hat{X} = (V \setminus \{v_1, v_2, \ldots, v_{t-1}\}, F)$. Thus $\hat{X}$ is a q-complementary k-hypergraph. Moreover,

$$\bigcap_{i=1}^{t-1} Aut(X)_{v_i} \leq Aut(\hat{X}).$$

Since the group $\bigcap_{i=1}^{t-1} Aut(X)_{v_i}$ acts transitively on $V(\hat{X}) = V \setminus \{v_1, v_2, \ldots, v_{t-1}\}$, it follows that $\hat{X}$ is vertex-transitive. The order of $\hat{X}$ is

$$|V \setminus \{v_1, v_2, \ldots, v_{t-1}\}| = n - t + 1$$

where $n - t + 1 \equiv 1 \pmod{q^{\ell+1}}$. Hence Theorem 2.3 implies that

$$p^{(n-t+1)_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \text{for every prime } p. \qquad \square$$

3 Constructions

In this section, we prove the sufficiency of condition (1) in Theorem 1.3. We begin with a construction of vertex-transitive q-complementary uniform hypergraphs of prime power order. These hypergraphs are 'Paley-like' in the sense that the construction uses similar algebraic tools to those used in the construction of the well known Paley graphs in [14], the generalized Paley graphs constructed in [8] and studied in [9], the Peisert graphs in [11], and the Paley uniform hypergraphs in [3, 6, 12].

If $\mathbb{F}$ is a finite field and $a_1, a_2, \ldots, a_k \in \mathbb{F}$, the *Van der Monde determinant* of $a_1, a_2, \ldots, a_k$ is defined as $VM(a_1, \ldots, a_k) = \prod_{i>j}(a_i - a_j)$.

Construction 3.1. Paley-like uniform hypergraph
Let q be an odd prime. Let k be an integer, and let n be a prime power such that $n \equiv 1 \pmod{q^{\ell+1}}$, where $\ell = \max\{k_{(q)}, (k-1)_{(q)}\}$. Let r be a divisor of $(n-1)/q^{\ell+1}$. Let $\mathbb{F}_n$ be the field of order n, and let ω be a generator of the multiplicative group $\mathbb{F}_n^*$. Let S denote the group of squares in $\mathbb{F}_n^*$, and let

$$c = \begin{cases} \gcd\left(n-1, r\binom{k}{2}\right), & n \text{ even} \\ \gcd\left(\frac{n-1}{2}, r\binom{k}{2}\right), & n \text{ odd} \end{cases}.$$

For $j = 0, 1, \ldots, qc - 1$, let F_j denote the coset $\omega^{2j} \left\langle \omega^{2qr\binom{k}{2}} \right\rangle$ in S. Finally, define $P_{n,k,r}$ to be the k-hypergraph with vertex set

$$V(P_{n,k,r}) := \mathbb{F}_n,$$

and edge set

$$E(P_{n,k,r}) := \{\{a_1, \ldots, a_k\} \in \mathbb{F}_n^{(k)} : VM^2(a_1, \ldots, a_k) \in F_0 \cup \cdots \cup F_{c-1}\}.$$

For $a \in \mathbb{F}_n^*$ and $b \in \mathbb{F}_n$, recall that $\alpha_{a,b} : \mathbb{F}_n \to \mathbb{F}_n$ denotes the bijection defined by $x^{\alpha_{a,b}} := ax + b$ for all $x \in \mathbb{F}_n$.

Lemma 3.2. Let $X = P_{n,k,r}$ denote the Paley-like k-hypergraph defined in Construction 3.1.

(1) Let $m' = \gcd \left(m \in \{1, 2, \ldots, p - 1\} \ : \ m\binom{k}{2} = sc \text{ where } q \nmid s \right)$. Then

    (a) $(Aut(X) \cup Ant_q(X)) \cap AGL_1(n) = \langle \alpha_{\omega^{m'},0}, \alpha_{1,1} \rangle$

    (b) $Aut(X) \cap AGL_1(n) = \langle \alpha_{\omega^{m'q},0}, \alpha_{1,1} \rangle$.

(2) (a) $\langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle \leq Aut(X)$

    (b) $\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle \leq Aut(X) \cup Ant_q(X)$

(3) X is vertex-transitive and q-complementary.

Proof: If n is odd, then $n - 1$ is even and so $|S| = (n - 1)/2$. Our choice of ℓ and r guarantee that the highest power of q that divides $\binom{k}{2}$ is ℓ, while the highest power of q that divides $(n - 1)/r$ is at least $\ell + 1$. This implies that

$$\left[\langle \omega^2 \rangle : \left\langle \omega^{2rq\binom{k}{2}} \right\rangle \right] = \gcd \left(\frac{n - 1}{2}, rq\binom{k}{2} \right) = q \gcd \left(\frac{n - 1}{2}, r\binom{k}{2} \right) = qc.$$

Similarly, if n is even, then $n - 1$ is odd, $|S| = n - 1$, and the highest power of q dividing $(n - 1)/r$ is at least $\ell + 1$. This implies that

$$\left[\langle \omega^2 \rangle : \left\langle \omega^{2rq\binom{k}{2}} \right\rangle \right] = \gcd \left(n - 1, rq\binom{k}{2} \right) = q \gcd \left(n - 1, r\binom{k}{2} \right) = qc.$$

Since $S = \langle \omega^2 \rangle$ whether n is even or odd, we have shown that, in both cases, the number of cosets of $\left\langle \omega^{2rq\binom{k}{2}} \right\rangle$ in $S = \langle \omega^2 \rangle$ is qc, and so $\{F_j\}_{j=0}^{qc-1}$ partitions S. Moreover, $\omega^{2s} F_j = F_{j+s(\bmod qc)}$ for any positive integer s.

For each $i = 0, 1, \ldots, q - 1$, let

$$A_i = F_{ic} \cup F_{ic+1} \cup F_{ic+2} \cup \cdots \cup F_{ic+(c-1)},$$

and let
$$E_i = \{\{a_1, a_2, \ldots, a_k\} \in \mathbb{F}_n^{(k)} : VM^2(a_1, a_2, \ldots, a_k) \in A_i\}.$$

Then $\{A_i\}_{i=0}^{q-1}$ partitions S, and $\omega^{2sc}A_i = A_{i+s(\bmod q)}$ for any integer s. Also, $\{E_i\}_{i=0}^{q-1}$ partitions $\mathbb{F}_n^{(k)}$, and $E = E(X) = E_0$. Observe that for any k-subset $\{a_1, \ldots a_k\} \in \mathbb{F}_n^{(k)}$ and any $b \in \mathbb{F}_n$, we have

$$VM^2(a_1 + b, a_2 + b, \ldots, a_k + b) = VM^2(a_1, a_2, \ldots, a_k).$$

It follows that $\alpha_{1,b} \in Aut(X)$ for all $b \in \mathbb{F}_n$, and so $\langle \alpha_{1,1} \rangle \le Aut(X)$.

Now we will find some more automorphisms and some q-antimorphisms of X.

(1) If m is an integer such that $m\binom{k}{2} = sc$ for an integer s such that $q \nmid s$, then

$$VM^2(\omega^m a_1, \ldots, \omega^m a_k) = \omega^{2m\binom{k}{2}}VM^2(a_1, \ldots, a_k) = \omega^{2sc}VM^2(a_1, \ldots, a_k).$$

Thus $\alpha_{\omega^m,0}$ maps each k-subset of $\mathbb{F}_n$ with square Van der Monde determinant in A_i to a k-subset of $\mathbb{F}_n$ with square Van der Monde determinant in $A_{i+s(\bmod q)}$ for each $i = 0, 1, \ldots, q - 1$. Hence the permutation $\theta = \alpha_{\omega^m,0}$ induces a mapping from E_i to $E_{i+s(\bmod q)}$ for each i. Since q does not divide s and q is prime, we have $\{E^{\theta^i}\}_{i=0}^{q-1} = \{E_{i+s(\bmod q)}\}_{i=0}^{q-1} = \{E_i\}_{i=0}^{q-1}$, which partitions $\mathbb{F}_n^{(k)}$. Thus θ is a q-antimorphism of X. Now Lemma 1.1(1) implies that

$$\alpha_{\omega^{mi},0} \in Ant_q(X) \quad \text{for all } i \not\equiv 0 \ (\bmod q),$$

and

$$\alpha_{\omega^{mi},0} \in Aut(X) \quad \text{for all } i \equiv 0 \ (\bmod q).$$

Now the composition of two automorphisms of X is again an automorphism of X, and the composition of a q-antimorphism of X with an automorphism of X is a q-antimorphism of X. Since $\langle \alpha_{1,1} \rangle \le Aut(X)$, it follows that

$$\langle \alpha_{\omega^m,0}, \alpha_{1,1} \rangle \le Aut(X) \cup Ant_q(X) \quad \text{and} \quad \langle \alpha_{\omega^{qm},0}, \alpha_{1,1} \rangle \le Aut(X)$$

for all $m \in M$. But $\langle \omega^m : m \in M \rangle$ is a cyclic group generated by $\omega^{m'}$, where $m' = \gcd(m : m \in M)$. Hence

$$\langle \alpha_{\omega^{m'},0}, \alpha_{1,1} \rangle \le Aut(X) \cup Ant_q(X) \quad \text{and} \quad \langle \alpha_{\omega^{qm'},0}, \alpha_{1,1} \rangle \le Aut(X).$$

Next we show that if $\alpha_{a,b} \in Aut(X) \cup Ant_q(X)$, then $a \in \langle \omega^{m'} \rangle$. Suppose that $a \notin \langle \omega^{m'} \rangle$. Now $\langle \omega^m \rangle \subseteq \langle \omega^{m'} \rangle$ for all $m \in M$. Hence we must have $a = \omega^z$ for an integer $z \notin M$. Observe that

$$VM^2(a_1^{\alpha_{a,b}}, \ldots, a_k^{\alpha_{a,b}}) = VM^2(\omega^z a_1 + b, \ldots, \omega^z a_k + b)$$
$$= \omega^{2z\binom{k}{2}}VM^2(a_1, \ldots, a_k).$$

Since $z \notin M$, $z\binom{k}{2}$ is *not* a multiple of c, and so $\alpha_{a,b}$ must *not* induce a permutation of the sets $E_0, E_1, \ldots, E_{q-1}$. Thus $\alpha_{a,b}$ is neither an automorphism nor a q-antimorphism of X. Hence if $a \notin \langle \omega^{m'} \rangle$, then $\alpha_{a,b} \notin Aut(X) \cup Ant_q(X)$. We conclude that

$$(Aut(X) \cup Ant_q(X)) \cap AGL_1(n) = \langle \alpha_{\omega^{m'},0}, \alpha_{1,1} \rangle$$

and

$$Aut(X) \cap AGL_1(n) = \langle \alpha_{\omega^{qm'},0}, \alpha_{1,1} \rangle,$$

as claimed.

(2) The highest power of q dividing $\binom{k}{2}$ is ℓ, and q^ℓ divides $(n-1)/r$ when n is odd, and it divides $(n-1)/2r$ when n is even. Since $c = \gcd\left(|S|, r\binom{k}{2}\right)$, this implies that $r\binom{k}{2} = sc$ for a positive integer s which is not divisible by q. Thus (2) follows directly from (1).

(3) Since the subgroup $\langle \alpha_{1,1} \rangle$ of $Aut(X)$ acts transitively on $\mathbb{F}_n = V(X)$, it follows that X is vertex-transitive, and since $Ant_q(X) \neq \emptyset$, the k-hypergraph X is q-complementary. $\square$

In Section 4.3, we will use some group theoretic results to find the complete set of automorphisms and q-antimorphisms of the Paley-like k-hypergraphs of Construction 3.1 which have prime order.

Lemma 3.2 shows that condition (1) of Theorem 1.3 is sufficient when n is a prime power. We now generalize Construction 3.1 and prove that this condition is sufficient for all n.

Construction 3.3. Generalized Paley-like uniform hypergraph

Let q be an odd prime, let k be an integer, and let n be a positive integer such that

$$p^{n_{(p)}} \equiv 1 \pmod{q^{\ell+1}} \quad \text{for every prime } p,$$

where ℓ is the largest positive integer such that q^ℓ divides a positive integer m with $m \leq k$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ be the unique prime factorization of n, where p_i is prime, $\alpha_i \geq 1$ and $p_1 < p_2 < \ldots < p_t$. For each $i \in \{1, 2, \ldots, t\}$, let $n_i = p_i^{\alpha_i}$, let r_i be a divisor of the integer $(n_i - 1)/q^{\ell+1}$, and let $r = (r_1, r_2, \ldots, r_t)$. Let $\mathbb{F}_{n_i}$ denote the field of order n_i. Let

$$V = \mathbb{F}_{n_1} \times \mathbb{F}_{n_2} \times \ldots \times \mathbb{F}_{n_t}.$$

Define a mapping $\zeta : V^{(k)} \to \mathbb{Z}_2$ by

$$\zeta(\{x_1, x_2, \ldots, x_k\}) = \begin{cases} 0 & \text{if } \{x_{1j}, x_{2j}, \ldots, x_{kj}\} \in E(P_{n_j, m, r_j}), \\ & \quad \text{where } j = \min\{1 \leq i \leq t : |\{x_{1i}, x_{2i}, \ldots, x_{ki}\}| > 1\} \\ & \quad \text{and } m = |\{x_{1j}, x_{2j}, \ldots, x_{kj}\}|. \\ 1 & \text{otherwise.} \end{cases}$$

Now define $X_{n,k,r}$ to be the k-hypergraph with vertex set V and edge set

$$E = \{\{x_1, x_2, \ldots, x_k\} \in V^{(k)} : \zeta(\{x_1, x_2, \ldots, x_k\}) = 0\}.$$

Note that when $t = 1$ and $n = n_1 = p_1^{\alpha_1}$ is a prime power congruent to 1 modulo $q^{\ell+1}$, the k-hypergraph $X_{n,k,r}$ of Construction 3.3 is the same as the Paley-like k-hypergraph P_{n_1,k,r_1} given by Construction 3.1.

Lemma 3.4. *The k-hypergraph $X_{n,k,r}$ defined in Construction* 3.3 *is vertex-transitive and q-complementary.*

Proof: Since $p^{n_{(p)}} \equiv 1 \pmod{q^{\ell+1}}$ for every prime p, it follows that for each i, $n_i \equiv 1 \pmod{q^{\ell+1}}$, and hence $n_i \equiv 1 \pmod{q^{b+1}}$ for all $b \leq \ell$. Now by definition, $\ell = \max\{\ell_m : 1 < m \leq k\}$ where $\ell_m = \max\{m_{(q)}, (m-1)_{(q)}\}$. Hence $n_i \equiv 1 \pmod{q^{\ell_m+1}}$ for $1 < m \leq k$, and so P_{n_i,m,r_i} is well defined for $1 \leq i \leq t$ and $1 < m \leq k$. Thus the edges of $X_{n,k,r}$ are well defined.

Let $\mathbb{F}_{n_i}^*$ denote the (cyclic) multiplicative group of nonzero elements in $\mathbb{F}_{n_i}$, and let ω_i be a generator of $\mathbb{F}_{n_i}^*$. For $1 \leq i \leq t$, define a bijection $\phi_i : \mathbb{F}_{n_i} \to \mathbb{F}_{n_i}$ by $x^{\phi_i} := \omega_i^{r_i} x$ for all $x \in \mathbb{F}_{n_i}$. Then by Lemma 3.2(3), $\phi_i \in Ant_q(P_{n_i,m,r_i})$ for $1 < m \leq k$, so it follows from the definition of $X_{n,k,r}$ that $(\phi_1, \phi_2, \ldots, \phi_t) \in Ant_q(X_{n,k,r})$. Hence $X_{n,k,r}$ is q-complementary.

Next we verify that $X_{n,k,r}$ is vertex-transitive. For $1 \leq i \leq t$, define a bijection $\alpha_i : \mathbb{F}_{n_i} \to \mathbb{F}_{n_i}$ by $x^{\alpha_i} := x + 1$, for all $x \in \mathbb{F}_{n_i}$. Then for each i, the mapping α_i preserves the Van der Monde determinant of any m pairwise distinct elements in $\mathbb{F}_{n_i}$, and hence α_i is an automorphism of P_{n_i,m,r_i}, for $1 < m \leq k$. Consequently

$$\langle \alpha_1 \rangle \times \langle \alpha_2 \rangle \times \cdots \times \langle \alpha_t \rangle \leq Aut(X_{n,k,r}).$$

Since $\langle \alpha_1 \rangle \times \langle \alpha_2 \rangle \times \cdots \times \langle \alpha_t \rangle$ acts transitively on $V = \mathbb{F}_{n_1} \times \mathbb{F}_{n_2} \times \cdots \times \mathbb{F}_{n_t}$, we conclude that $X_{n,k,r}$ is vertex-transitive. $\square$

Proof of Theorem 1.3: The necessity of condition (1) follows directly from Theorem 2.3. The sufficiency of condition (1) was proved for the prime $q = 2$ in [3], so we may assume that q is an odd prime. Since $k = bq^\ell$ or $k = bq^\ell + 1$ for some positive integer $b < q$, for any integer m such that $1 < m \leq k$ we have $\ell \geq m_{(q)}$. Thus k, ℓ, and n satisfy the hypotheses of Construction 3.3, and so the sufficiency of condition (1) follows from Construction 3.3 and Lemma 3.4 whenever q is an odd prime. $\square$

4 Vertex-transitive q-complementary hypergraphs of prime order

4.1 Preliminaries - some group theory

In Section 4.3, we will characterize the vertex-transitive q-complementary k-hypergraphs of prime order p in the cases where k or $k - 1$ is equal to bq^ℓ for a positive integer $b < q$, and $p \equiv 1 \pmod{q^{\ell+1}}$. To do this, we will require some results from group theory.

The following two theorems due to Burnside [16] and Zassenhaus [17] restrict the automorphism group of a vertex-transitive k-hypergraph of prime order.

Theorem 4.1. (Burnside [16]) *If G is a transitive permutation group acting on a prime number p of elements, then either G is doubly-transitive or*

$$G \equiv \{\alpha_{a,b} : a \in H \leq \mathbb{F}_p^* , \ b \in \mathbb{F}_p\}.$$

Theorem 4.2. (Zassenhaus [17, 4]) *A sharply doubly-transitive permutation group of prime degree p is equivalent as a permutation group to $AGL_1(p)$.*

4.2 Generating q-complementary hypergraphs

Given a (q, k)-complementing permutation θ, we may generate all of the q-complementary k-hypergraphs for which θ is a q-antimorphism in the following way. Let $c_0, c_1, \ldots, c_{q-1}$ be q colors and suppose we have the complete set of orbits of θ on $V^{(k)}$, each of the form $A, A^\theta, A^{\theta^2}, \ldots$. Within each of these orbits, color the elements of the form A^{θ^s} with color c_i if and only if $s \equiv i \pmod{q}$. Suppose there are m orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ of θ on $V^{(k)}$. If we fix a color c_{i_j} in the j-th orbit and then choose elements of $V^{(k)}$ of color c_{i_j} from orbit $\mathcal{O}_j$ for an edge set E, for each $j = 1, 2, \ldots, m$, then $X = (V, E)$ is q-complementary with q-antimorphism θ. There are q^m choices for the list of colors $c_{i1}, c_{i2}, \ldots, c_{im}$, and hence we can use this method to generate the set of all q^m q-complementary k-hypergraphs for which θ is a q-antimorphism. This set is called the θ-*switching class* of q-complementary k-hypergraphs on V, since we can obtain one from another by switching the edges of one colour for another colour in each orbit in some subset of the orbits of θ on $V^{(k)}$, and two hypergraphs in this θ-switching class are called θ-*switching equivalent.*

4.3 A characterization

Now we are ready to characterize the structure of the vertex-transitive q-complementary k-hypergraphs of odd prime order p in the cases where q is an odd prime, $k = bq^\ell$ or $k = bq^\ell + 1$ for a positive integer $b < q$, and $p \equiv 1 \pmod{q^{\ell+1}}$. We will show that these hypergraphs are θ-switching equivalent to a Paley-like hypergraph of Construction 3.1, for some permutation θ. We begin by determining the set of possible automorphisms and q-antimorphisms of these hypergraphs.

Lemma 4.3. *Let q be an odd prime, let ℓ and b be positive integers with $b < q$, and suppose that k or $k - 1$ is equal to bq^ℓ. If X is a vertex-transitive q-complementary k-hypergraph of odd prime order $p \equiv 1 \pmod{q^{\ell+1}}$, then $Aut(X) \cup Ant_q(X)$ is equivalent as a permutation group to a subgroup of $AGL_1(p)$. That is*

$$Aut(X) \cup Ant_q(X) \equiv \{\alpha_{a,b} : a \in G \leq \mathbb{F}_p^* , \ b \in \mathbb{F}_p\}.$$

Proof: Since X is vertex-transitive, $Aut(X)$ and $Aut(X) \cup Ant_q(X)$ are both transitive permutation groups acting on a prime number of elements. Since $p \equiv 1 \pmod{q^{\ell+1}}$, Lemma 1.2 implies that X is not doubly-transitive, and so by Burnside's Theorem,

$$Aut(X) \equiv \{\alpha_{a,b} : a \in H \leq \mathbb{F}_p^* , \ b \in \mathbb{F}_p\} \tag{4}$$

for some subgroup H of $\mathbb{F}_p^*$. Now since $AGL_1(p)$ is doubly-transitive and X is not doubly-transitive, $Aut(X) \not\equiv AGL_1(p)$. Hence H is a proper subgroup of $\mathbb{F}_p^*$ in Equation (4). Hence $|H| < p - 1$, and so

$$|Aut(X)| = p|H| = \frac{p(p-1)}{d} \quad \text{for an integer } d \geq 2. \tag{5}$$

Since $Aut(X)$ is an index-q subgroup of $Aut(X) \cup Ant_q(X)$, we also have

$$|Aut(X) \cup Ant_q(X)| = q|Aut(X)| = \frac{q}{d}p(p-1). \tag{6}$$

If $Aut(X) \cup Ant_q(X)$ is not doubly-transitive, then the result follows directly from Burnside's Theorem 4.1. On the other hand, if $Aut(X) \cup Ant_q(X)$ is doubly-transitive, then the Orbit-Stabilizer Lemma guarantees that $p(p-1)$ divides $|Aut(X) \cup Ant_q(X)|$. Hence $|Aut(X) \cup Ant_q(X)| = mp(p-1)$ for a positive integer m, and (6) implies that $m = \frac{q}{d}$. If the integer d in (5) satisfies $2 \leq d < q$, then as q is prime, $d \nmid q$, contradicting the fact that m is an integer. We conclude that $d \geq q$. Now the fact that $1 \leq m = \frac{q}{d}$ implies that $d = q$ and $m = 1$. Hence $|Aut(X) \cup Ant_q(X)| = p(p-1)$, and so $Aut(X) \cup Ant_q(X)$ must be sharply doubly-transitive. Hence Zassenhaus' Theorem 4.2 implies that $Aut(X) \cup Ant_q(X) \equiv AGL_1(p)$. $\qquad\square$

In the next lemma, we find the complete set of automorphisms and q-antimorphisms of the Paley-like k-hypergraphs of Construction 3.1 which have prime order.

Lemma 4.4. *Let q be an odd prime, let b and ℓ be positive integers such that $b < q$, and suppose that k or $k - 1$ is equal to bq^ℓ. Let p be a prime such that $p \equiv 1 \pmod{q^{\ell+1}}$. Let r be a divisor of $\frac{p-1}{q^{\ell+1}}$, and let $X = P_{p,k,r}$ be the Paley-like k-hypergraph defined in Construction 3.1. Let $c = \gcd\left(\frac{p-1}{2}, r\binom{k}{2}\right)$. Then*

$$Aut(X) \cup Ant_q(X) = \langle \alpha_{\omega^{m'},0}, \alpha_{1,1} \rangle \quad \text{and} \quad Aut(X) = \langle \alpha_{\omega^{qm'},0}, \alpha_{1,1} \rangle,$$

for $m' = \gcd\left(m \in \{1, 2, \ldots, p-1\} \; : \; m\binom{k}{2} = sc \text{ where } q \nmid s\right).$

Proof: Since p is prime, Lemma 4.3 implies that

$$Aut(X) \cup Ant_q(X) \leq AGL_1(p),$$

while Lemma 3.2 implies that

$$(Aut(X) \cup Ant_q(X)) \cap AGL_1(p) = \langle \alpha_{\omega^{m'},0}, \alpha_{1,1} \rangle$$

and

$$Aut(X) \cap AGL_1(p) = \langle \alpha_{\omega^{qm'},0}, \alpha_{1,1} \rangle,$$

so the result follows. $\qquad\square$

Theorem 4.5.

Let q be an odd prime, and suppose $X = (V, E)$ is a vertex-transitive q-complementary k-hypergraph of prime order p, where k or $k - 1$ is equal to bq^ℓ for a positive integer $b < q$, and $p \equiv 1 \pmod{q^{\ell+1}}$. Let ω be a generator of $\mathbb{F}_p$. Then X is isomorphic to a k-hypergraph Y with vertex set $\mathbb{F}_p$ for which $Aut(Y) = \langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle \leq Aut(P_{p,k,r})$ and $Aut(Y) \cup Ant_q(Y) = \langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle \leq Aut(P_{p,k,r}) \cup Ant_q(P_{p,k,r})$, where $r = p(p - 1)/|Aut(X) \cup Ant_q(X)|$. Consequently Y is θ-switching equivalent to $P_{p,k,r}$ for all $\theta \in \{\alpha_{\omega^{mr},b} : q \nmid m, b \in \mathbb{F}_p\}$.

Proof: By Lemma 4.3, there is $\varphi : V \to \mathbb{F}_p$ such that $Y = (\varphi(V), \varphi(E))$ satisfies

$$Aut(Y) \cup Ant_q(Y) = \{\alpha_{a,b} : a \in G \leq \mathbb{F}_p^* , \ b \in \mathbb{F}_p\},$$

and $Aut(Y)$ is an index-q subgroup of this group, so

$$Aut(Y) = \{\alpha_{a,b} : a \in K \leq \mathbb{F}_p^* , \ b \in \mathbb{F}_p\},$$

where K is an index-q subgroup of G. Since

$$r = \frac{p(p-1)}{|Aut(Y) \cup Ant_q(Y)|} = \frac{p(p-1)}{|Aut(X) \cup Ant_q(X)|}$$

and ω is a generator of $\mathbb{F}_p^*$, it follows that the set G of multiplicative permutations in $Aut(Y) \cup Ant_q(Y)$ is $\langle \omega^r \rangle$, and the set K of multiplicative automorphisms of Y is $\langle \omega^{qr} \rangle$. If we can verify that r is a divisor of $\frac{(p-1)}{q^{\ell+1}}$, then $P_{p,k,r}$ exists and Lemma 3.2(4) guarantees that $Aut(Y) = \langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle \leq Aut(P_{p,k,r})$ and $Aut(Y) \cup Ant_q(Y) = \langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle \leq Aut(P_{p,k,r}) \cup Ant_q(P_{p,k,r})$, as claimed.

It remains to show that $r = \frac{p(p-1)}{|Aut(X) \cup Ant_q(X)|}$ is a divisor of $(p - 1)/q^{\ell+1}$. First we will show that both of the integers p and q^ℓ divide $|Aut(Y)|$. We have $Aut(Y) = \langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle$, which contains the subgroup $\langle \alpha_{1,1} \rangle$ of order p, and so p divides $|Aut(Y)|$. Now by Lemma 1.1(3), Y has a q-antimorphism θ with order a power of q, and Lemma 2.1 guarantees that θ has one fixed point and every nontrivial orbit of θ has length divisible by $q^{\ell+1}$. Thus $|\theta|$ is divisible by $q^{\ell+1}$, and so $|Aut(Y) \cup Ant_q(Y)| = q|Aut(Y)|$ is divisible by $q^{\ell+1}$. It follows that q^ℓ divides $|Aut(Y)|$. Since $p \equiv 1 \pmod{q^{\ell+1}}$, the primes p and q are not equal, and so pq^ℓ divides $|Aut(X)|$.

Now observe that

$$r = \frac{p(p-1)}{|Aut(X) \cup Ant_q(X)|} = \frac{p(p-1)}{|Aut(Y) \cup Ant_q(Y)|} = \frac{p(p-1)q^{\ell+1}}{q|Aut(Y)|q^{\ell+1}}$$

which implies that

$$\frac{p-1}{q^{\ell+1}} = r \left(\frac{|Aut(Y)|}{pq^\ell} \right). \tag{7}$$

Since pq^ℓ divides $|Aut(X)|$, the quotient $\frac{|Aut(Y)|}{pq^\ell}$ is an integer. Hence Equation (7) implies that r divides the integer $\frac{p-1}{q^{\ell+1}}$. This completes the proof. $\qquad \square$

4.4 Generating transitive q-complementary k-hypergraphs

In this section, we present an algorithm for generating all vertex-transitive q-complement-ary k-hypergraphs of prime order $p \equiv 1 \pmod{q^{\ell+1}}$, whenever q is an odd prime and k or $k-1$ is equal to bq^ℓ for a positive integer $b < q$. We use the fact that such hypergraphs are $\alpha_{\omega^r,0}$-switching equivalent to the Paley-like hypergraph $P_{p,k,r}$, for some r.

Algorithm 4.6.
Let q be an odd prime, let ℓ and b be positive integers with $b < q$, and suppose that k or $k-1$ is equal to bq^ℓ. Let p be a prime such that $p \equiv 1 \pmod{q^{\ell+1}}$. Let ω be a generator of $\mathbb{F}_p^*$. Let $c_0, c_1, c_2, \ldots, c_{q-1}$ denote q colors. In Step 1(a)-(b) we will color the elements of $\mathbb{F}_p^{(k)}$ with these q colors.

1. Choose a divisor r of $(p-1)/2^{\ell+1}$, let $P_{p,k,r}$ be the Paley-like k-hypergraph of order p, and let $\theta = \alpha_{\omega^r,0}$.

   (a) Take an uncolored edge $A \in E(P_{p,k,r})$ In Steps (i), (ii) and (iii) below, we will find and color the orbit $\mathcal{O} = A^{\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle}$ of the group $\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle$ on $\mathbb{F}_p^{(k)}$ which contains A.

      (i) Create a sequence of elements of $\mathbb{F}_p^{(k)}$

      $$A, \quad A^\theta, \quad A^{\theta^2}, \quad A^{\theta^3}, \quad \ldots, \quad A^{\theta^{|\theta|-1}}. \tag{8}$$

      For each $i = 0, 1, \ldots, q-1$, color the elements of the form A^{θ^s} with color c_i if and only if $s \equiv i \pmod{q}$.

      (ii) Repeat Step 1(a)(i) but replace A with the first element of $A^{\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle}$ which is uncolored.

      (iii) Repeat Step 1(a)(ii) until all elements of $A^{\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle}$ have been colored.

   (b) Repeat Step 1(a) until all edges of $P_{p,k,r}$ have been colored. (Then all edges of $\mathbb{F}_p^{(k)}$ have been colored.)

   (c) Let m be the number of orbits of the group $\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle$ on $\mathbb{F}_p^{(k)}$ created in Steps 1(a) and 1(b), and choose an ordering $\mathcal{O}_{A_1}, \mathcal{O}_{A_2}, \ldots, \mathcal{O}_{A_m}$ of these orbits, where $A_j \in E(P_{p,k,r})$ for $j = 1, 2, \ldots, m$.

      (i) Choose a vector $v \in \mathbb{Z}_q^m$, and let X_v^r be the k-hypergraph with vertex set $\mathbb{F}_p$ and edge set E, where an edge $e \in \mathcal{O}_{A_j}$ is in E if and only if e is colored c_i and $v_j = i$, for some i. (Note that $P_{p,k,r} = X_\mathbf{0}^r$.)

      (ii) Repeat Step 2(c)(i) for all vectors $v \in \mathbb{Z}_q^m$.

2. Repeat Step 1 for all divisors r of $(p-1)/q^{\ell+1}$.

Theorem 4.7. *Let q be an odd prime, let b and ℓ be positive integers such that $b < q$, and suppose that $k = bq^\ell$ or $k = bq^\ell + 1$. Let p be a prime such that $p \equiv 1 \pmod{q^{\ell+1}}$, and let X be a k-hypergraph of order p. Then X is a vertex-transitive and q-complementary if and only if X is isomorphic to a k-hypergraph generated by Algorithm 4.6.*

Proof: ($\Rightarrow$) Suppose that X is a vertex transitive self-complementary k-hypergraph of order p. By Theorem 4.5, X is isomorphic to a k-hypergraph Y with vertex set $\mathbb{F}_p$ for which $Aut(Y) = \langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle \leq Aut(P_{p,k,r})$ and $Aut(Y) \cup Ant_q(Y) = \langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle \leq Aut(P_{p,k,r}) \cup Ant_q(P_{p,k,r})$, where $r = p(p-1)/|Aut(X) \cup Ant(X)|$. We will obtain Y from $P_{p,k,r}$ using Algorithm 4.6.

Since $\alpha_{\omega^r,0}$ is a q-antimorphism of Y, Y is $\alpha_{\omega^r,0}$-switching equivalent to $P_{p,k,r}$. Since $P_{p,k,r} = X_{\mathbf{0}}^r$, $E(P_{p,k,r})$ consists of all of the edges of color c_0. Hence Y can be obtained from $P_{p,k,r}$ by exchanging the edges of color c_0 for edges of another color in each orbit in some subset of the orbits of $\alpha_{\omega^r,0}$ on $V^{(k)}$. Moreover, since $Aut(Y) = \langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle$, for each $i \in \{0, 1, \ldots, q-1\}$ the set of orbits from which we chose edges of color c_i for $E(Y)$ must also be equal to a union of orbits of $\langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle$ on $\mathbb{F}_p^{(k)}$. This implies that Y can be obtained from $P_{p,k,r}$ by exchanging edges of color c_0 for edges of another color, say c_{i_j}, in each orbit $\mathcal{O}_{A_j}$ in a subset $\mathcal{S}$ of the orbits $\mathcal{O}_{A_1}, \mathcal{O}_{A_2}, \ldots, \mathcal{O}_{A_m}$ constructed in Steps 1(a)-(b) of Algorithm 4.6. Let $v \in \mathbb{Z}_q^m$ be the vector such that $v_j = i$ if and only if $A_j \in \mathcal{S}$ and the edges of $E(Y) \cap \mathcal{O}_{A_j}$ have color c_i. Then $Y = X_v^r$. Since $X \cong Y$, we have $X \cong X_v^r$, and so X is isomorphic to a k-hypergraph generated by Algorithm 4.6.

($\Leftarrow$) Suppose that X is a k-hypergraph of order p that is isomorphic to a k-hypergraph generated by Algorithm 4.6. We will show that X is vertex transitive and q-complementary. Now $X \cong X_v^r = (V, E)$ for some divisor r of $(p-1)/q^{\ell+1}$ and some $v \in \mathbb{Z}_q^m$, where m is the number of orbits of the group $\langle \alpha_{\omega^r,0}, \alpha_{1,1} \rangle$ on $\mathbb{F}_p^{(k)}$. The k-hypergraph X_v^r is constructed by choosing the edges of color c_{v_j} from each of the orbits $\mathcal{O}_{A_j}$ in $\{\mathcal{O}_{A_1}, \mathcal{O}_{A_2}, \ldots, \mathcal{O}_{A_m}\}$. Our coloring method in Step 1(a) guarantees that, for each $i = 1, 2, \ldots, q-1$, the set of edges of color c_i in the orbit $\mathcal{O}_{A_j}$ constitutes an orbit of $\langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle$ on $\mathbb{F}_p^{(k)}$, for each $j \in \{1, 2, \ldots, m\}$. This implies that $\langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle \leq Aut(X_v^r)$. Since $\langle \alpha_{1,1} \rangle \leq \langle \alpha_{\omega^{qr},0}, \alpha_{1,1} \rangle$, and $\langle \alpha_{1,1} \rangle$ acts transitively on $\mathbb{F}_p$, we conclude that $Aut(X_v^r)$ acts transitively on $V(X_v^r) = \mathbb{F}_p$, and so X_v^r is vertex-transitive.

Now let $E_{i,j}$ denote the set of edges of color c_i in the orbit $\mathcal{O}_{A_j}$. Our coloring method in Step 1(a) guarantees that $\{E_{i,j}^{\theta^i}\}_{i=0}^{q-1}$ partitions the edges of $\mathcal{O}_{A_j}$, where $\theta = \alpha_{\omega^r,0}$, for each $j \in \{1, 2, \ldots, m\}$. Consequently $\{E^{\theta^i}\}_{i=0}^{q-1}$ partitions $V^{(k)}$. This implies that $\alpha_{\omega,0} \in Ant_q(X_v^r)$, and so X_v^r is q-complementary.

Hence X_v^r is a vertex-transitive q-complementary k-hypergraph of order p, and since $X \cong X_v^r$, so is X. $\qquad\square$

5 Open problem

When $t = q = 2$, Theorem 1.4 gives necessary conditions on the order of a doubly-transitive self-complementary k-hypergraph in the cases where $k = 2^\ell$ or $k = 2^\ell + 1$.

Corollary 5.1. *Let ℓ be a positive integer, let $k = 2^\ell$ or $k = 2^\ell + 1$, and suppose $n \equiv 2 \pmod{2^{\ell+1}}$. If there exists a doubly-transitive self-complementary k-hypergraph of order*

n, then

$$p^{(n-1)_{(p)}} \equiv 1 \pmod{2^{\ell+1}} \quad \textit{for every prime } p.$$

$\square$

In [13], Potočnik and Šajna gave a construction for doubly-transitive self-complementary 3-hypergraphs which show that the necessary conditions of Corollary 5.1 are sufficient in the case where $k = 3$ and n is a prime power. This leads the author to pose the following open problem.

Problem 5.2. *Determine the values of t, q and k for which condition (2) of Theorem 1.4 is sufficient for the existence of a t-fold-transitive q-complementary k-hypergraph.*

The 3-hypergraphs of prime power order constructed in [13] are the only known doubly-transitive self-complementary 3-hypergraphs. It would be interesting to know whether any others exist.

References

[1] C.J. Colbourn and J.H. Dinitz (editors), *Handbook of Combinatorial Designs*, Chapman and Hall/CRC Press, Boca Raton, Florida (2007).

[2] S. Gosselin, Cyclically t-complementary uniform hypergraphs (2009). To appear.

[3] S. Gosselin, Vertex-transitive self-complementary uniform hypergraphs of prime order, *Discrete Math.* **310** (2010), 671-680.

[4] M. Hall Jr., *The Theory of Groups*. Macmillan, New York, 1959.

[5] G.B. Khosrovshahi and B. Tayfeh-Rezaie, Root cases of large sets of t-designs, *Discrete Math.* **263** (2003), 143-155.

[6] W. Kocay, Reconstructing graphs as subsumed graphs of hypergraphs, and some self-complementary triple systems, *Graphs Combin.* **8** (1992), 259-276.

[7] C.H. Li and C.E. Praeger, On partitioning the orbitals of a transitive permutation group. *Trans. Amer. Math. Soc.* **355** (2003), 637-653.

[8] C.H. Li, T.K. Lim and C.E. Praeger, Homogeneous factorizations of complete graphs with edge-transitive factors. *J. Algebraic Combin.* **29** (2009), 107-132.

[9] T.K. Lim and C.E. Praeger, On generalized Paley graphs and their automorphism groups. *Michigan Math. J.* **58** (2009), 293-308.

[10] M. Muzychuk, On Sylow subgraphs of vertex-transitive self-complementary graphs, *Bull. London Math. Soc.* **31** (1999), 531-533.

[11] W. Peisert, All self-complementary symmetric graphs, *J. Algebra* **240** (2001), 209-229.

[12] P. Potočnik and M. Šajna, Vertex-transitive self-complementary uniform hypergraphs. *European J. Combin.* **30** (2009), 327-337.

[13] P. Potočnik and M. Šajna, Self-complementary two-graphs and almost self-complementary double covers, *European J. Combin.* **28** (2007), 1561-1574.

[14] S.B. Rao, On regular and strongly-regular self-complementary graphs, *Discrete Math.* **54** (1985), 73-82.

[15] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t. *Discrete Math.,* **65** (1987), 301-311.

[16] H. Wielandt, *Finite Permutation Groups.* Academic Press, New York (1964).

[17] H. Zassenhaus, Über endliche Fastkörper. *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 187-220.