Vertex-transitive self-complementary uniform hypergraphs of prime order

Shonda Gosselin*
Department of Mathematics and Statistics, University of Winnipeg
515 Portage Avenue, Winnipeg, MB R3B 2E9, CANADA
E-mail: s.gosselin@uwinnipeg.ca
Phone: 011+1-204-786-9346
Fax: 011+1-204-774-4134

7th September 2009

Abstract

For an integer n and a prime p, let $n_{(p)} = \max\{i : p^i \text{ divides } n\}$. In this paper, we present a construction for vertex-transitive self-complementary k-uniform hypergraphs of order n for each integer n such that $p^{n_{(p)}} \equiv 1 \pmod{2^{\ell+1}}$ for every prime p, where $\ell = \max\{k_{(2)}, (k-1)_{(2)}\}$ and consequently we prove that the necessary conditions on the order of vertex-transitive self-complementary uniform hypergraphs of rank $k = 2^\ell$ or $k = 2^\ell + 1$ due to Potoňick and Šajna are sufficient. In addition, we use Burnside's characterization of transitive groups of prime degree to characterize the structure of vertex-transitive self-complementary k-hypergraphs which have prime order p in the case where $k = 2^\ell$ or $k = 2^\ell + 1$ and $p \equiv 1 \pmod{2^{\ell+1}}$, and we present an algorithm to generate all of these structures. We obtain a bound on the number of distinct vertex-transitive self-complementary graphs of prime order $p \equiv 1 \pmod 4$, up to isomorphism.

Key words: Self-complementary hypergraph; Uniform hypergraph; Transitive hypergraph; Complementing permutation; Large set of t-designs
AMS Subject Classification Codes: 05C65, 05B05 05E20, 05C85.

1 Introduction

1.1 Definitions

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

*Supported by an NSERC PGS D.

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. Note that 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 $V(X)$.

The *complement* X^C of a k-hypergraph $X = (V, E)$ is the hypergraph with vertex set V and edge set $V^{(k)} \setminus E$. A k-hypergraph X is called *self-complementary* if it is isomorphic to its complement. An isomorphism between a self-complementary k-hypergraph $X = (V, E)$ and its complement X^C is called an *antimorphism* of X. The set of all antimorphisms of X will be denoted by $Ant(X)$. It is easy to check that $Aut(X) \cup Ant(X)$ is a subgroup of $Sym(V)$, and that $Aut(X)$ is an index-2 subgroup of $Aut(X) \cup Ant(X)$. Also, it is clear that $Aut(X) = Aut(X^C)$ when X is self-complementary.

Let $X = (V, E)$ be a k-hypergraph, let t be a positive integer. A k-hypergraph X is called *t-subset-regular* if the 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 *doubly-transitive* if $Aut(X)$ acts transitively on the set of ordered pairs of distinct vertices of X. Clearly, every vertex-transitive k-hypergraph is 1-subset-regular and every doubly-transitive k-hypergraph is 2-subset-regular.

1.2 Connection to design theory

There is a connection between t-subset-regular hypergraphs and designs. Hence results from design theory are applicable to these hypergraphs and vice versa. A *t-(n, k, λ) design* is a pair $(V, \mathcal{B})$ in which V is a set of cardinality n and $\mathcal{B}$ is a collection of k-subsets of a point set V, such that every t-subset of V is contained in exactly λ elements of $\mathcal{B}$. Hence a t-subset-regular k-hypergraph X of order n is a t-(n, k, λ) design in which λ is equal to the t-valency of X. A *large set of t-(n, k, λ) designs* of size N, denoted by $LS[N](t, k, n)$, is a partition of the complete design $V^{(k)}$ into N disjoint t-(n, k, λ) designs, where $\lambda = \binom{n-t}{k-t}/N$. If a t-subset regular k-hypergraph X of order n is self-complementary, then X and its complement X^C are both t-(n, k, λ) designs with $\lambda = \binom{n-t}{k-t}/2$. Hence the pair $\{X, X^C\}$ is an $LS[2](t, k, n)$ in which the t-designs are isomorphic. If X is vertex-transitive or doubly-transitive, then the corresponding t-design is point-transitive or 2-point-transitive, respectively. Hence vertex-transitive self-complementary k-hypergraphs of order n correspond bijectively to large sets of t-designs $LS[2](t, k, n)$ for some $t \geq 1$ 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

Teirlink's remarkable proof in [9] 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 this paper, we will use terminology from hypergraph theory, rather than design theory.

1.3 Notation

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. 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 $\tau^{-1}G\tau$ 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 conjugate of G by τ, respectively. For finite sets U and V, and any permutation $\alpha \in Sym(U)$ and $\beta \in Sym(V)$, the permutation $\alpha \times \beta \in Sym(U \times V)$ is defined by $(u,v)^{\alpha\times\beta} = (u^\alpha, v^\beta)$, for all $(u,v) \in U \times V$.

1.4 Necessary conditions on order

The following result is actually a corollary to a more general result due to Khosrovshahi and Tayfeh-Rezaie in [4], which gives necessary conditions on the order of large sets of t-designs, and it was first noted by Potočnik and Šajna in [7].

Theorem 1.1. [7] *Suppose that $k = 2^\ell$ or $k = 2^\ell + 1$ for some positive integer ℓ, and that X is a self-complementary k-hypergraph of order n. Let t be a positive integer such that $1 \le t < k$. If X is t-subset regular, then $n \equiv j \pmod{2^{\ell+1}}$ for some $j \in \{t, t+1, \ldots, k-1\}$.*

Since vertex-transitive self-complementary k-hypergraphs are necessarily 1-subset-regular, we can use Theorem 1.1 to find basic necessary conditions on their order in the case where $k = 2^\ell$ or $k = 2^\ell + 1$. However, the following result due to Potočnik and Šajna [7] shows that the condition of transitivity implies stronger necessary conditions on the order of these structures in the case where $n \equiv 1 \pmod{2^{\ell+1}}$.

Theorem 1.2. [7] *Let ℓ be a positive integer, let $k = 2^\ell$ or $k = 2^\ell + 1$, and let $n \equiv 1 \pmod{2^{\ell+1}}$. If there exists a vertex-transitive self-complementary k-hypergraph of order n, then*

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

It has been shown that the necessary conditions of Theorem 1.2 are sufficient in the case where $k = 2$ [8], $k = 3$ and n is odd [7], and where n is a prime power [7]. In Section 2, we will present a construction to prove that the necessary conditions of Theorem 1.2 are sufficient in all cases. In Section 3, we will characterize the structure of vertex-transitive self-complementary k-hypergraphs which have prime order p in the cases where $k = 2^\ell$ or $k = 2^\ell + 1$, and $p \equiv 1 (\mathrm{mod}\ 2^{\ell+1})$.

2 Constructions

We begin with a construction of vertex-transitive self-complementary uniform hypergraphs of prime power order. 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 2.1. ***Paley* k-*uniform hypergraph***
Let k be an integer, $k \geq 2$, and let q be a prime power such that $q \equiv 1 (\mathrm{mod}\ 2^{\ell+1})$, where $\ell = \max\{k_{(2)}, (k-1)_{(2)}\}$. Let r be a divisor of the integer $(q-1)/2^{\ell+1}$. Let $\mathbb{F}_q$ be the field of order q, let ω be a generator of the multiplicative group $\mathbb{F}_q^*$, and let $c = gcd(n-1, r\binom{k}{2})$. For $i = 0, 1, \ldots, 2c-1$, let F_i denote the coset $\omega^i \left\langle \omega^{2r\binom{k}{2}} \right\rangle$ in $\mathbb{F}_q^*$. Finally, define $P_{q,k,r}$ to be the k-hypergraph with vertex set

$$V(P_{q,k,r}) := \mathbb{F}_q,$$

and edge set

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

It should be noted that Potočnik and Šajna first introduced Construction 2.1 [7] with $r = 1$. Their construction was in turn an extension of the well-known construction of Paley graphs, which can be found in Rao [8]. The extension to Paley 3-hypergraphs with $r = 1$ had been previously introduced by Kocay in [5]. Peisert also presented this construction in [6] in the case where $k = 2$ and r is any divisor of $(q-1)/4$.

Lemma 2.2. *The Paley k-hypergraph $P_{q,k,r}$ defined in Construction 2.1 is a vertex-transitive and self-complementary k-hypergraph.*

Proof: Since r divides $(q-1)/2^{\ell+1}$, we have $q - 1 = 2^{\ell+1}rt$ for some positive integer t. Let d be the order of $\omega^{r\binom{k}{2}}$ in $\mathbb{F}_q^*$. Then

$$d = \frac{q-1}{gcd(q-1, r\binom{k}{2})}.$$

First consider the case when k is even. Then $k = 2^\ell k'$ for k' odd. Hence

$$\begin{aligned} d &= \frac{2^{\ell+1}rt}{gcd(2^{\ell+1}rt, rk(k-1)/2)} = \frac{2^{\ell+1}t}{\gcd(2^{\ell+1}t, 2^\ell k'(k-1)/2)} \\ &= \frac{2^{\ell+1}t}{\gcd(2^{\ell+1}t, 2^{\ell-1}k'(k-1))} = 4\left(\frac{t}{\gcd(4t, k'(k-1))}\right). \end{aligned}$$

Since k' and $k-1$ are both odd integers, $\gcd(4t, k'(k-1))$ is a divisor of t, and so $t/\gcd(4t, k'(k-1))$ is an integer. Thus d is divisible by 4 when k is even. Now suppose that k is odd. Then $k-1 = 2^\ell k'$ where k' is odd. We similarly obtain

$$d = 4\left(\frac{t}{\gcd(4t, kk')}\right), \tag{1}$$

and since k and k' are both odd, it follows that d is divisible by 4 when k is odd also.

Thus d is divisible by 4, and consequently the subgroup $\left\langle \omega^{2r\binom{k}{2}} \right\rangle$ is of even order and even index in $\mathbb{F}_q^*$. Hence $-1 \in \left\langle \omega^{2r\binom{k}{2}} \right\rangle$, and so the edge set of $P_{q,k,r}$ is well defined. Also, the sets

$$A := \bigcup_{i=0}^{c-1} \omega^i \left\langle \omega^{r\binom{k}{2}} \right\rangle = \bigcup_{i=0}^{c-1} F_i$$

and

$$\bar{A} := \bigcup_{i=0}^{c-1} \omega^{i+r\binom{k}{2}} \left\langle \omega^{2r\binom{k}{2}} \right\rangle = \bigcup_{i=c}^{2c-1} F_i = \omega^{r\binom{k}{2}} A$$

partition $\mathbb{F}_q^*$.

Define a bijection $\phi : \mathbb{F}_q \to \mathbb{F}_q$ by $a^\phi := \omega^r a$, for all $a \in \mathbb{F}_q$. Observe that for any k-subset $\{a_1, \ldots a_k\} \in \mathbb{F}_q^{(k)}$, we have

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

Thus ϕ induces a mapping from A to $\bar{A}$, and hence from $E(P_{q,k,r})$ to $E(P^C_{q,k,r}) = \mathbb{F}_q^{(k)} \setminus E(P_{q,k,r})$. Thus ϕ is an antimorphism of $P_{q,k,r}$, and so $P_{q,k,r}$ is a self-complementary k-hypergraph.

To see that $P_{q,k,r}$ is vertex-transitive, it suffices to show that an automorphism can map 0 to any other vertex. For any $a \in \mathbb{F}_q$, the bijection $\alpha : \mathbb{F}_q \to \mathbb{F}_q$ defined by $y^\alpha = y + a$, for all $y \in \mathbb{F}_q$, maps 0 to a. Since

$$VM(a_1 + a, \ldots, a_k + a) = VM(a_1, \ldots, a_k),$$

the bijection α is an automorphism of $P_{q,k,r}$, and so $P_{q,k,r}$ is vertex-transitive. □

In Section 3 we will use results from group theory to find the complete automorphism group of the Paley k-hypergraph $P(q,k,r)$ of Construction 2.1, in the case where q is prime and $k = 2^\ell$ or $k = 2^\ell + 1$.

Lemma 2.2 shows that the converse of Theorem 1.2 holds when n is a prime power. We now generalize Construction 2.1 and prove that the converse of Theorem 1.2 is true in all cases.

Construction 2.3. *Let k be an integer, $k \geq 2$, and let n be a positive integer such that*

$$p^{n_{(p)}} \equiv 1 \pmod{2^{\ell+1}} \quad \textit{for every prime } p,$$

where ℓ is the largest positive integer such that 2^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 $q_i = p_i^{\alpha_i}$, let r_i be a divisor of the integer $(q_i - 1)/2^{\ell+1}$, and let $r = (r_1, r_2, \ldots, r_t)$. Let $\mathbb{F}_{q_i}$ denote the field of order q_i.

Let

$$V = \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \ldots \times \mathbb{F}_{q_{t-1}} \times \mathbb{F}_{q_t}.$$

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

$$\zeta(\{x_1, x_2, \ldots, x_k\}) =$$

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

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 $n = q_1 = p_1^{\alpha_1}$ is a prime power congruent to 1 modulo $2^{\ell+1}$, the k-hypergraph $X_{n,k,r}$ of Construction 2.3 is the same as the k-hypergraph P_{q_1,k,r_1} given by Construction 2.1.

Lemma 2.4. *The k-hypergraph $X_{n,k,r}$ defined in Construction 2.3 is vertex-transitive and self-complementary.*

Proof: Since $p^{n_{(p)}} \equiv 1 \pmod{2^{\ell+1}}$ for every prime p, it follows that for each i, $q_i \equiv 1 \pmod{2^{\ell+1}}$, and hence $q_i \equiv 1 \pmod{2^{b+1}}$ for all $b \leq \ell$. Now by definition, $\ell = \max\{\ell_m : 1 < m \leq k\}$ where $\ell_m = \max\{m_{(2)}, (m-1)_{(2)}\}$. Hence $q_i \equiv 1 \pmod{2^{\ell_m+1}}$ for $1 < m \leq k$, and so P_{q_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 $\mathbb{F}_{q_i}^*$ denote the (cyclic) multiplicative group of non-zero elements in $\mathbb{F}_{q_i}$, and let ω_i be a generator of $\mathbb{F}_{q_i}^*$. For each $1 \leq i \leq t$, define a bijection $\phi_i : \mathbb{F}_{q_i} \to \mathbb{F}_{q_i}$ by $a^{\phi_i} := \omega_i^{r_i} a$, for all $a \in \mathbb{F}_n$. Then $\phi_i \in Ant(P_{q_i,m,r_i})$ for $1 < m \leq k$, so it follows from the definition of $X_{n,k,r}$ that $\phi_1 \times \phi_2 \times \cdots \times \phi_t \in Ant(X_{n,k,r})$. Hence $X_{n,k,r}$ is self-complementary.

To see that $X_{n,k,r}$ is vertex-transitive, it suffices to show that an automorphism can map the vertex $\mathbf{0} := (0, 0, \ldots, 0)$ to any other vertex. For $1 \leq i \leq t$ and for any $x_i \in \mathbb{F}_{q_i}$, the bijection $\alpha_{x_i} : \mathbb{F}_{q_i} \to \mathbb{F}_{q_i}$ defined by $y^\alpha = y + x_i$, for all $y \in \mathbb{F}_{q_i}$, maps 0 to x_i. Moreover, α_{x_i} preserves the Van der Monde determinant of any m pairwise distinct elements in $\mathbb{F}_{q_i}$, and hence α_{x_i} is an automorphism of P_{q_i,m,r_i}, for $1 < m \leq k$. Now let $\mathbf{x} = (x_1, x_2, \ldots, x_t) \in V$. It follows from the

definition of $X_{n,k,r}$ that $\alpha_{\mathbf{x}} := \alpha_{x_1} \times \alpha_{x_2} \times \cdots \times \alpha_{x_t} \in Aut(X_{n,k,r})$. Since $\alpha_{\mathbf{x}}$ maps $\mathbf{0}$ to $\mathbf{x}$ and $\mathbf{x}$ was an arbitrary element of V, it follows that $Aut(X_{n,k,r})$ acts transitively on V, and so $X_{n,k,r}$ is vertex-transitive. □

Theorem 2.5. *Let ℓ be a positive integer, let $k = 2^\ell$ or $k = 2^\ell + 1$, and let $n \equiv 1 \pmod{2^{\ell+1}}$. There exists a vertex-transitive self-complementary k-hypergraph of order n if and only if*

$$p^{n_{(p)}} \equiv 1 (\mathrm{mod}\ 2^{\ell+1}) \quad \textit{for every prime } p. \tag{2}$$

Proof: The necessity of condition (2) follows directly from Theorem 1.2. Since $k = 2^\ell$ or $k = 2^\ell + 1$, for any integer m such that $1 < m \leq k$, ℓ is greater than or equal to the largest integer i such that 2^i divides m. Thus k, ℓ, and n satisfy the hypotheses of Construction 2.3, and so the sufficiency of condition (2) follows from Lemma 2.4. □

3 Vertex-transitive self-complementary uniform hypergraphs of prime order

3.1 Preliminaries - some group theory

In Section 3.3, we will characterize the vertex-transitive self-complementary k-hypergraphs of prime order p in the cases where $k = 2^\ell$ or $k = 2^\ell + 1$ and $p \equiv 1 (\mathrm{mod} 2^{\ell+1})$. To do this, we will require some results from group theory.

For a prime power q, let $\mathbb{F}_q^*$ denote the multiplicative group of units of the finite field $\mathbb{F}_q$ of order q. Given $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, define the mapping $T_{a,b}$ by $T_{a,b} : x \to ax + b$. One can show that $T_{a,b}$ is a permutation of $\mathbb{F}_q$, and that $\{T_{a,b} : a \in \mathbb{F}_q^*\ ,\ b \in \mathbb{F}_q\}$ is a group, called the *affine linear group of permutations* acting on $\mathbb{F}_q$. This group will be denoted by $AGL_1(q)$. 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 $g \in G$ such that $\alpha^g = \beta$. The group G is *sharply doubly-transitive* if G is sharply transitive in its action on ordered pairs of distinct elements from Ω.

The following two theorems due to Burnside [10] and Zassenhaus [11] restrict the automorphism group of a vertex-transitive k-hypergraph of prime order.

Theorem 3.1. (Burnside [10]) *If G is a transitive permutation group acting on a prime number p of elements, then either G is doubly-transitive or*

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

Theorem 3.2. (Zassenhaus [11, 3]) *A sharply doubly-transitive permutation group of prime degree p is equivalent as a permutation group to $AGL_1(p)$.*

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

Lemma 3.3. (Orbit-stabilizer [10]) *Let G be a permutation group acting on V and let x be a point in V. Then $|G| = |G_x||x^G|$.*

3.2 Complementing permutations

In some of the literature (eg. [5]), a permutation which is an antimorphism of a self-complementary k-hypergraph is called a *k-complementing permutation*, and we have the following natural characterization.

Lemma 3.4. [5]

A permutation θ on V is a k-complementing permutation

$\iff$ *$A^{\theta^j} \neq A$, $\forall\ A \in V^{(k)}, \forall\ j$ odd,*

$\iff$ *the sequence $A, A^\theta, A^{\theta^2}, A^{\theta^3}, \ldots$ has even length, $\forall\ A \in V^{(k)}$.*

If θ is a k-complementing permutation in $Sym(V)$, the set of self-complementary k-hypergraphs on V for which θ is an antimorphism is called the *θ-switching class* of self-complementary k-hypergraphs on V. Two self-complementary k-hypergraphs in this θ-switching class are said to be *θ-switching equivalent*.

We will require the following lemma due to Potočnik and Šajna. It is proved within their proof of Theorem 1.2 in [7].

Lemma 3.5. [7] *Let ℓ be a positive integer, let $k = 2^\ell$ or $k = 2^\ell + 1$, and let $n \equiv 1 \pmod{2^{\ell+1}}$. Let $\mathcal{O}_2$ be the set of k-complementing permutations in $Sym(n)$ whose orders are powers of 2. Then every element of $\mathcal{O}_2$ has exactly one fixed point and all other orbits have length divisible by $2^{\ell+1}$.*

3.3 A characterization

Now we are ready to characterize the vertex-transitive self-complementary k-hypergraphs of prime order p in the cases where $k = 2^\ell$ or $k = 2^\ell + 1$, and $p \equiv 1 \pmod{2^{\ell+1}}$. We begin by determining the set of possible automorphisms and antimorphisms of these hypergraphs.

Lemma 3.6. *Suppose $k = 2^\ell$ or $k = 2^\ell + 1$. If X is a vertex-transitive self-complementary k-hypergraph of prime order $p \equiv 1 \pmod{2^{\ell+1}}$, then $Ant(X) \cup Aut(X)$ is equivalent as a permutation group to a subgroup of $AGL_1(p)$. That is*

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

Proof: Since X is vertex-transitive, $Aut(X)$ and $Ant(X) \cup Aut(X)$ are both transitive permutation groups acting on a prime number of elements. Since $p \equiv 1 \pmod{2^{\ell+1}}$, Theorem 1.1 implies that X is not doubly-transitive, and so by Burnside's Theorem,

$$Aut(X) \equiv \{T_{a,b} : a \in H \leq \mathbb{F}_p^*\ ,\ b \in \mathbb{F}_p\} \tag{3}$$

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 (3), and so $|H| \leq \frac{p-1}{2}$. Thus $|Aut(X)| = p|H| \leq \frac{p(p-1)}{2}$. Since $Aut(X)$ is an index-2 subgroup of $Aut(X) \cup Ant(X)$, we have $|Aut(X) \cup |Ant(X)| = 2|Aut(X)| \leq p(p-1)$.

If $Aut(X) \cup Ant(X)$ is not doubly-transitive, then the result follows from Burnside's Theorem 3.1. On the other hand, if $Aut(X) \cup Ant(X)$ is doubly-transitive, then certainly $|Aut(X) \cup Ant(X)| \geq p(p-1)$, which implies that $|Aut(X) \cup Ant(X)| = p(p-1)$. Hence $Aut(X) \cup Ant(X)$ must be sharply doubly-transitive, and so in this case the result follows from Zassenhaus' Theorem 3.2. □

In the next lemma, we completely determine the set of automorphisms and antimorphisms of the Paley k-hypergraphs of Construction 2.1 which have prime order.

Lemma 3.7. *Let ℓ be a positive integer. Suppose $k = 2^\ell$ or $k = 2^\ell + 1$, and q be a prime power such that $q \equiv 1 \pmod{2^{\ell+1}}$. Let r be a divisor of $\frac{q-1}{2^{\ell+1}}$, and let $X = P_{q,k,r}$ be the Paley k-hypergraph defined in Construction 2.1. Let $c = \gcd(q-1, r\binom{k}{2})$.*

(1) Let s be an integer such that $s\binom{k}{2}$ is an odd multiple of c. Then

- *(a) $\langle T_{\omega^{2s},0}, T_{1,1}\rangle \leq Aut(X)$.*
- *(b) $\langle T_{\omega^s,0}, T_{1,1}\rangle \leq Aut(X) \cup Ant(X)$.*

(2) $\langle T_{\omega^{2r},0}, T_{1,1}\rangle \leq Aut(X)$ and $\langle T_{\omega^r,0}, T_{1,1}\rangle \leq Aut(X) \cup Ant(X)$.

(3) If q is prime, then $Aut(X) \cup Ant(X) = \langle T_{\omega^{s'},0}, T_{1,1}\rangle$, where

$$s' = \gcd\left(s : s \in \{1, 2, \ldots, q-1\}, s\binom{k}{2} \text{ is a multiple of } c\right).$$

Proof:

(1) Suppose that $s\binom{k}{2} = (2m+1)c$. First we will show that $\omega^{s\binom{k}{2}}A = \bar{A}$. Note that $\omega^i F_j = F_{(i+j)_{[2c]}}$. We have

$$\omega^{s\binom{k}{2}}A = \bigcup_{i=0}^{c-1} \omega^{(2m+1)c}F_i = \bigcup_{i=0}^{c-1} F_{(i+(2m+1)c)_{[2c]}} = \bigcup_{i=0}^{c-1} F_{i+c} = \bigcup_{i=c}^{2c-1} F_i = \bar{A}.$$

Hence $\omega^{s\binom{k}{2}}A = \bar{A}$. This implies that, for any element $x \in \mathbb{F}_q^*$, we have

$$x \in A \iff \omega^{(2m+1)s\binom{k}{2}}x \in \bar{A} \text{ and } \omega^{(2m)s\binom{k}{2}}x \in A$$

for every integer m.

(a) Now observe that for a k-subset $\{a_1, a_2, \ldots, a_k\} \in \mathbb{F}_q^{(k)}$, an integer m, and an element $b \in \mathbb{F}_q$, we have

$$VM(\omega^{2ms}a_1 + b, \ldots, \omega^{2ms}a_k + b) = \omega^{(2m)s\binom{k}{2}} VM(a_1, \ldots, a_k).$$

Thus the permutation $T_{\omega^{2ms},b}$ maps the Van der Monde determinant of an element of $\mathbb{F}_q^{(k)}$ from A to A, or from $\bar{A}$ to $\bar{A}$. It follows that $T_{\omega^{2ms},b}$ is an automorphism of X. Since m and b were chosen arbitrarily, we conclude that $\langle T_{\omega^{2s},0}, T_{1,1}\rangle \leq Aut(X)$.

(b) Observe that for a k-subset $\{a_1, \ldots a_k\} \in \mathbb{F}_q^{(k)}$, an integer m, and an element $b \in \mathbb{F}_q$, we have

$$VM(\omega^{(2m+1)s}a_1 + b, \ldots, \omega^{(2m+1)s}a_k + b) = \omega^{(2m+1)s\binom{k}{2}} VM(a_1, \ldots, a_k).$$

It follows that the permutation $T_{\omega^{(2m+1)s},b}$ maps the Van der Monde determinant of an element of $\mathbb{F}_q^{(k)}$ from A to $\bar{A}$, or vice versa. Hence $T_{\omega^{(2m+1)s},b}$ induces a mapping from $E(X)$ to $E(X^C) = \mathbb{F}_q^{(k)} \setminus E(X)$. Thus $T_{\omega^{(2m+1)s},b}$ is an antimorphism of X. Since m and b were chosen arbitrarily, we conclude that $\{T_{\omega^{(2m+1)s},b} : m \in \mathbb{Z},\ b \in \mathbb{F}_q\} \subseteq Ant(X)$. This implies that $\langle T_{\omega^s,0}, T_{1,1}\rangle \leq Aut(X) \cup Ant(X)$.

(2) Observe that

$$\left|\omega^{r\binom{k}{2}}\right| = \frac{q-1}{\gcd(q-1, r\binom{k}{2})} = \frac{q-1}{c}.$$

Since c divides $q-1$, we also have $|\omega^c| = (q-1)/c$. Since the cyclic subgroup of $\mathbb{F}_q^*$ of order $(q-1)/c$ is unique, it follows that $\left\langle \omega^{r\binom{k}{2}} \right\rangle = \langle \omega^c \rangle$. Thus $r\binom{k}{2} = mc$ for an integer m such that $\gcd((q-1)/c, m) = 1$. The proof of Lemma 2.2 shows that $(q-1)/c$ is divisible by 4, and hence even, and thus the integer m must be odd. Hence $r\binom{k}{2}$ is an odd multiple of c, and so the result follows from Part (1).

(3) Let $S = \{s \in \{1, 2, \ldots, q-1\} : s\binom{k}{2}$ is a multiple of $c\}$. Part (1) implies that

$$\langle T_{\omega^s,0}, T_{1,1}\rangle \leq Aut(X) \cup Ant(X)$$

for all $s \in S$. It follows that

$$\{T_{a,b} : a \in \langle \omega^s : s \in S\rangle, b \in \mathbb{F}_q\} \leq Aut(X) \cup Ant(X). \tag{4}$$

But $\langle \omega^s : s \in S\rangle$ is a cyclic group generated by $\omega^{s'}$, where $s' = \gcd(s : s \in S)$. Hence (4) implies that

$$\langle T_{\omega^{s'},0}, T_{1,1}\rangle \leq Aut(X) \cup Ant(X).$$

Now if q is prime, Lemma 3.6 implies that $Aut(X) \cup Ant(X) \leq AGL_1(q)$. Thus it remains to show that if $T_{a,b} \in Aut(X) \cup Ant(X)$, then $a \in \langle \omega^{s'} \rangle$.

Suppose that $a \notin \langle \omega^{s'} \rangle$. Now $\langle \omega^s \rangle \subseteq \langle \omega^{s'} \rangle$ for all $s \in S$. If $a = \omega^m$ for an integer m such that $m\binom{k}{2}$ is a multiple of c, then $a \in S$, and so $a \in \langle \omega^{s'} \rangle$, giving a contradiction. Hence $a = \omega^n$ for an integer n such that $n\binom{k}{2}$ is *not* a multiple of c. Consequently $\omega^{n\binom{k}{2}} A \neq A$ and $\omega^{n\binom{k}{2}} A \neq \bar{A}$. Hence $T_{a,b} \notin Aut(X) \cup Ant(X)$. It follows that $(Aut(X) \cup Ant(X)) \cap AGL_1(q) = \langle T_{\omega^{s'},0}, T_{1,1} \rangle$ and hence $(Aut(X) \cup Ant(X)) = \langle T_{\omega^{s'},0}, T_{1,1} \rangle$, as claimed.

□

Theorem 3.8.
Suppose $X = (V, E)$ is a vertex-transitive self-complementary k-hypergraph of prime order p, where $k = 2^\ell$ or $k = 2^\ell + 1$ and $p \equiv 1 \pmod{2^{\ell+1}}$. 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 $Aut(Y) = \langle T_{\omega^{2r},0}, T_{1,1} \rangle \leq Aut(P_{p,k,r})$ and $Ant(Y) \cup Aut(Y) = \langle T_{\omega^r,0}, T_{1,1} \rangle \leq Ant(P_{p,k,r}) \cup Aut(P_{p,k,r})$, where $r = p(p-1)/|Aut(X) \cup Ant(X)|$. Consequently, Y is in the θ-switching class of $P_{p,k,r}$ for every permutation $\theta \in \{T_{\omega^{rm},b} : m \text{ odd}, b \in \mathbb{F}_p\}$.

Proof: By Lemma 3.6,

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

and $Aut(X)$ is an index-2 subgroup of this group, so

$$Aut(X) \equiv \{T_{a,b} : a \in K \leq \mathbb{F}_p^* \ , \ b \in \mathbb{F}_p\},$$

where K is an index-2 subgroup of G. Thus there is $\varphi : V \to \mathbb{F}_p$ such that $Y = (\varphi(V), \varphi(E))$ satisfies

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

and

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

Now $|Ant(Y) \cup Aut(Y)|$ is even, and its order divides $p(p-1)$. Since

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

and ω is a generator of $\mathbb{F}_p^*$, it follows that the set G of multiplicative permutations in $Ant(Y) \cup Aut(Y)$ is $\langle \omega^r \rangle$, and the set K of multiplicative automorphisms of Y is $\langle \omega^{2r} \rangle$. If we can verify that r is a divisor of $\frac{(p-1)}{2^{\ell+1}}$, then $P_{p,k,r}$ exists and $Aut(Y) = \langle T_{\omega^{2r},0} T_{1,1} \rangle \leq Aut(P_{p,k,r})$ and $Ant(Y) \cup Aut(Y) = \langle T_{\omega^r,0}, T_{1,1} \rangle \leq Ant(P_{p,k,r}) \cup Aut(P_{p,k,r})$. Consequently, Y is in the θ-switching class of $P_{p,k,r}$ for every $\theta \in \langle T_{\omega^r,0}, T_{1,1} \rangle \setminus \langle T_{\omega^{2r},0}, T_{1,1} \rangle = \{T_{\omega^{rm},b} : m \text{ odd}, b \in \mathbb{F}_p\}$.

It remains to show that $r = \frac{p(p-1)}{|Aut(X) \cup Ant(X)|}$ is a divisor of $(p-1)/2^{\ell+1}$. First we will show that both of the integers p and 2^ℓ divide $|Aut(Y)|$. We

have $Aut(Y) = \{T_{a,b} : a \in K \leq \mathbb{F}_p^* \ , \ b \in \mathbb{F}_p\}$, which contains the subgroup $\{T_{1,b} : b \in \mathbb{F}_p\}$ of order p, and so p divides $|Aut(Y)|$. Now let $\theta \in Ant(Y)$. Then θ has even order in $Ant(Y) \cup Aut(Y)$, so $|\theta| = 2^j s$ for some positive integer j and some odd positive integer s. Now $\theta^s \in Ant(Y)$ and θ^s has order 2^j, so Lemma 3.5 implies that θ^s has exactly one fixed point, and all other orbits of θ^s have length divisible by $2^{\ell+1}$. Hence the order of the antimorphism θ^s is divisible by $2^{\ell+1}$, and so $|Aut(Y) \cup Ant(Y)| = 2|Aut(Y)|$ is divisible by $2^{\ell+1}$. It follows that 2^ℓ divides $|Aut(Y)|$.

Now observe that

$$r = \frac{p(p-1)}{|Aut(X) \cup Ant(X)|} = \frac{p(p-1)}{|Aut(Y) \cup Ant(Y)|} = \frac{p(p-1)2^{\ell+1}}{2|Aut(Y)|2^{\ell+1}}$$
$$\implies \frac{p-1}{2^{\ell+1}} = r\left(\frac{|Aut(Y)|}{p2^\ell}\right). \tag{5}$$

Since $|Aut(Y)|$ is divisible by the odd prime p, and $|Aut(Y)|$ is also divisible by 2^ℓ, it follows that $\frac{|Aut(Y)|}{p2^\ell}$ is an integer. Hence Equation (5) implies that r divides the integer $\frac{p-1}{2^{\ell+1}}$. This completes the proof. □

3.4 Generating transitive k-hypergraphs

In this section, we will present an algorithm for generating all vertex-transitive self-complementary k-hypergraphs of prime order $p \equiv 1 \pmod{2^{\ell+1}}$, when $k = 2^\ell$ or $k = 2^\ell + 1$.

Algorithm 3.9.
Let ℓ be a positive integer, and suppose that $k = 2^\ell$ or $k = 2^\ell + 1$. Let p be a prime such that $p \equiv 1 \pmod{2^{\ell+1}}$. Let ω be a generator of $\mathbb{F}_p^*$.

1. Choose a divisor r of $(p-1)/2^{\ell+1}$, and let $\theta = T_{\omega^r,0}$.

   (a) Take an arbitrary uncolored element A of $\mathbb{F}_p^{(k)}$. In steps (i), (ii) and (iii) below, we will find the orbit $\mathcal{O}_A$ of the group $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(k)}$ which contains A.

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

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

      Colour the elements of the form $A^{\theta^{2i}}$ red and those of the form $A^{\theta^{2i+1}}$ blue.

      (ii) Repeat Step 1(a)(i) but replace A with the first element of $\mathbb{F}_p^{(k)}$ in the sequence

      $$A^{T_{1,1}}, A^{T_{1,1}^2}, \ldots, A^{T_{1,1}^{p-1}} \tag{6}$$

      which is uncolored.

(iii) Repeat Step 1(a)(ii) until all elements in the sequence (6) have been colored.

(b) Repeat Step 1(a) until all of the elements of $\mathbb{F}_p^{(k)}$ have been colored.

(c) Let m be the number of orbits of the group $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(k)}$ created in Step 1(a), and choose an ordering $\mathcal{O}_{A_1}, \mathcal{O}_{A_2}, \ldots, \mathcal{O}_{A_m}$ of these orbits.

(i) Choose a vector $v \in \mathbb{Z}_2^m$, and let X_v^r be the k-hypergraph with vertex set $\mathbb{F}_p$ and edge set E, where an edge $e \in \mathcal{O}_{A_i}$ is in E if and only if e is red and $v_i = 1$, or e is blue and $v_i = 0$.

(ii) Repeat step 2(b)(i) for all vectors $v \in \mathbb{Z}_2^m$.

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

Theorem 3.10. *Let ℓ be a positive integer, let $k = 2^\ell$ or $k = 2^\ell + 1$, and let p be a prime such that $p \equiv 1 \pmod{2^{\ell+1}}$. Let X be a k-hypergraph of order p. Then X is a vertex-transitive self-complementary if and only if X is isomorphic to a k-hypergraph generated by Algorithm 3.9.*

Proof: ($\Rightarrow$) Suppose that X is a vertex transitive self-complementary k-hypergraph of order p. By Theorem 3.8, X is isomorphic to a k-hypergraph Y with vertex set $\mathbb{F}_p$ for which $Aut(Y) = \langle T_{\omega^{2r},0}, T_{1,1}\rangle \leq Aut(P_{p,k,r})$ and $Ant(Y) \cup Aut(Y) = \langle T_{\omega^r,0}, T_{1,1}\rangle \leq Ant(P_{p,k,r}) \cup Aut(P_{p,k,r})$, where $r = p(p-1)/|Aut(X) \cup Ant(X)|$. We will obtain Y from $P_{p,k,r}$ using Algorithm 3.9.

First we show that $P_{p,k,r}$ is generated by Algorithm 3.9. Let $v \in \mathbb{Z}_2^m$ be the vector such that $v_i = 1$ if and only if $A_i \in E(P_{p,k,r})$, for all $i \in \{1, 2, \ldots, m\}$. Then $P_{p,k,r} = X_v^r$.

Now we will show how Y can be generated by Algorithm 3.9 from $P_{p,k,r}$. Now Y is in the θ-switching class of $P_{p,k,r}$ for every permutation $\theta \in \{T_{\omega^{rm},b} : m \text{ odd}, b \in \mathbb{F}_p\}$. In particular, Y is $T_{\omega,0}$-switching equivalent to $P_{p,k,r}$. That is, Y can be obtained from $P_{p,k,r}$ by changing edges to nonedges, and vice versa, in some collection S of orbits of $T_{\omega,0}$ on $\mathbb{F}_p^{(k)}$. Moreover, since $Aut(Y) = \langle T_{\omega^{2r},0}, T_{1,1}\rangle$, the collection S must also be equal to a union of orbits of $\langle T_{\omega^{2r},0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(k)}$. Hence S is a union of orbits of $\langle T_{\omega^r,0}, T_{\omega^{2r},0}, T_{1,1}\rangle = \langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(k)}$. This implies that Y can be obtained from $P_{p,k,r}$ by changing edges to nonedges, and vice versa, in a subset $\mathcal{S}$ of the orbits $\mathcal{O}_{A_1}, \mathcal{O}_{A_2}, \ldots, \mathcal{O}_{A_m}$ given by Algorithm 3.9. Let $w \in \mathbb{Z}_2^m$ be the vector such that $w_i = 1$ if and only if $A_i \in \mathcal{S}$. Then $Y = X_{v+w}^r$. Since $X \cong Y$, we have $X \cong X_{v+w}^r$, and so X is isomorphic to a k-hypergraph generated by Algorithm 3.9.

($\Leftarrow$) Suppose that X is a k-hypergraph of order p that is isomorphic to a k-hypergraph generated by Algorithm 3.9. We will show that X is vertex transitive and self-complementary. Now $X \cong X_v^r$ for some divisor r of $(p-1)/2^{\ell+1}$ and some $v \in \mathbb{Z}_2^m$, where m is the number of orbits of the group $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(k)}$. The k-hypergraph X_v^r is constructed by choosing either the red or the blue edges from each of the orbits in $\{\mathcal{O}_{A_1}, \mathcal{O}_{A_2}, \ldots, \mathcal{O}_{A_m}\}$. Our coloring method in

step 1(a) guarantees that each of the set of red edges and the set of blue edges in $\mathcal{O}_{A_i}$ constitutes an orbits of $\langle T_{\omega^2,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(k)}$, for all $i \in \{1,2,\ldots,m\}$. This implies that $\langle T_{\omega^2,0}, T_{1,1}\rangle \leq Aut(X_v^r)$. Since $\langle T_{1,1}\rangle \leq \langle T_{\omega^2,0}, T_{1,1}\rangle$, and $\langle T_{1,1}\rangle$ 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. Our coloring method in step 1(a) also guarantees that $T_{\omega,0}$ maps red edges onto blue edges, and vice versa, in the orbit $\mathcal{O}_{A_i}$, for all $i \in \{1,2,\ldots,m\}$. This implies that $T_{\omega,0} \in Ant(X_v^r)$, and so X_v^r is self-complementary.

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

When $k = 2$ or $k = 3$, Theorem 1.1 guarantees that for every vertex-transitive self-complementary k-hypergraph of prime order p, we must have $p \equiv 1 \pmod 4$. Hence Algorithm 3.9 generates *every* vertex-transitive self-complementary graph and 3-hypergraph of prime order.

Corollary 3.11. *For any prime $p \equiv 1 \pmod 4$, there are at most*

$$\sum_{r|\left(\frac{p-1}{4}\right)} 2^{r-1}$$

distinct vertex-transitive self-complementary graphs of order p, up to isomorphism.

Proof: Let r be a divisor of $(p-1)/4$. Then $\gcd(p-1, r) = r$. For each $i = 0, 1, \ldots, 2r-1$, let $\mathcal{E}_i = \{e \in \mathbb{F}_p^{(2)} : VM(e) \in \omega^i\langle\omega^{2r}\rangle\}$. We will prove that each of the orbits of the group $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(2)}$ has the form $\mathcal{E}_i \cup \mathcal{E}_{i+r}$, for some $i = 0, 1, \ldots, r-1$. For a given divisor r of $(p-1)/4$, Algorithm 3.9 generates at most 2^{m-1} pairwise non-isomorphic graphs X with $Aut(X) \cup Ant(X) = \langle T_{\omega^r,0}, T_{1,1}\rangle$, where m is the number of orbits of $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(2)}$. Finding these orbits explicitly will lead us to conclude that $m = r$ for each divisor r of $(p-1)/4$, and so the result will follow.

Now each element of $\{T_{\omega^{rm},b} : m \text{ odd}, b \in \mathbb{F}_p\}$ maps edges of $\mathcal{E}_i$ to edges of $\mathcal{E}_{i+r}$, where addition of subscripts is addition modulo $2r$. Also, each element of $G = \langle T_{\omega^{2r},0}, T_{1,1}\rangle$ maps edges of $\mathcal{E}_i$ to edges of $\mathcal{E}_i$. This implies that each orbit of $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(2)}$ is contained in $\mathcal{E}_i \cup \mathcal{E}_{i+r}$, for some $i \in \{0, 1, \ldots, r-1\}$.

Next we prove that $\langle T_{\omega^r,0}, T_{1,1}\rangle$ acts transitively on $\mathcal{E}_i \cup \mathcal{E}_{i+r}$, for all $i = 0, 1, \ldots, r-1$. It suffices to show that $G = \langle T_{\omega^{2r},0}, T_{1,1}\rangle$ acts transitively on the set of edges $\mathcal{E}_i$, for all $i = 0, 1, \ldots, 2r-1$. We have $|G| = p(p-1)/2r$. Now fix $\{x, y\} \in \mathbb{F}_p^{(2)}$. Recall that the group $AGL_1(p)$ acting on $\mathbb{F}_p$ is sharply doubly transitive. Since $G \leq AGL_1(p)$, it follows that at most two permutations in G fix $\{x, y\}$. Hence by the orbit-stabilizer Lemma 3.3, we obtain

$$|\{x, y\}^G| = |G|/|G_{\{x,y\}}| \geq |G|/2 = p(p-1)/4r. \tag{7}$$

Also, for integers i and j such that $0 \leq i, j \leq 2r-1$, we have $|\mathcal{E}_i| = |\mathcal{E}_j|$. This

implies that each of the edge sets $\mathcal{E}_i$ has size

$$|\mathcal{E}_i| = |\mathbb{F}_p^{(2)}|/2r = p(p-1)/4r. \tag{8}$$

Now (7) and (8) together imply that

$$|\{x,y\}^G| \geq |\mathcal{E}_i|, \quad \text{for all } i \in \{0,1,\ldots,2r-1\}. \tag{9}$$

Since each orbit of G on $\mathbb{F}_p^{(2)}$ is contained in $\mathcal{E}_i$ for some i, and (9) implies that each orbit of G on $\mathbb{F}_p^{(2)}$ has cardinality at least $|\mathcal{E}_i|$ for all i, it follows that each orbit of G on $\mathbb{F}_p^{(2)}$ is equal to $\mathcal{E}_i$ for some i. Hence G acts transitively on the set of edges $\mathcal{E}_i$, for all $i = 0,1,\ldots,2r-1$. This implies that $\langle T_{\omega^r,0}, T_{1,1}\rangle$ acts transitively on $\mathcal{E}_i \cup \mathcal{E}_{i+r}$, for all $i = 0,1,\ldots,2r-1$.

Since each orbit of $\langle T_{\omega^r,0}, T_{1,1}\rangle$ is contained in $\mathcal{E}_i \cup \mathcal{E}_{i+r}$ for some i, the fact that $\langle T_{\omega^r,0}, T_{1,1}\rangle$ acts transitively on $\mathcal{E}_i \cup \mathcal{E}_{i+r}$ implies that each orbit of $\langle T_{\omega^r,0}, T_{1,1}\rangle$ on $\mathbb{F}_p^{(2)}$ is equal to $\mathcal{E}_i \cup \mathcal{E}_{i+r}$ for some $i = 0,1,\ldots,r-1$. There are exactly r such orbits, and so $m = r$ in step 1(c) of Algorithm 3.9. Thus for each divisor r of $(p-1)/4$, Algorithm 3.9 generates exactly $|\mathbb{Z}_2^r| = 2^r$ vertex transitive self-complementary graphs of order p. Now every graph generated by the algorithm is isomorphic to its complement, which is also generated by the algorithm. It follows that there are at most

$$\sum_{r|\frac{p-1}{4}} 2^{r-1}$$

distinct vertex transitive self-complementary graphs of order p, up to isomorphism. □

4 Open Problems

When neither k nor $k-1$ is a power of 2, not much is known about the order of vertex-transitive k-uniform hypergraphs. However, using Burnside's Theorem, one may solve the following problem by examining the structure of doubly-transitive permutation groups.

Problem 4.1. *Let p be prime, and let k be a positive integer, $k \leq p-1$. Characterize the structure of vertex-transitive self-complementary k-uniform hypergraphs of order p.*

In [2], Dobson proved the following analogue to Burnside's characterization of transitive groups of prime degree, for transitive groups of prime power degree.

Theorem 4.2. *[2] A transitive group of odd prime-power degree such that every minimal transitive subgroup is cyclic is either doubly transitive (and hence known) or contains a normal Sylow p-subgroup.*

One may use Dobson's theorem to prove an analogue to Theorem 3.8 for uniform hypergraphs of prime power order. The author poses the following problem.

Problem 4.3. *Characterize the structure of vertex-transitive self-complementary k-uniform hypergraphs of prime power order.*

In the case where the rank $k = 2^\ell$ or $k = 2^\ell + 1$, and the order $n = p^r \equiv 1 \pmod{2^{\ell+1}}$, Theorem 1.1 implies that such a k-hypergraph X cannot be doubly-transitive, and so if the automorphism group of X contains a cycle of length p^r, then it contains a normal Sylow p-subgroup. Examining the structure of such groups may lead to a partial solution to Problem 4.3.

References

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

[2] E. Dobson, On groups of prime power degree that contain a full cycle, *Discrete Math.* **299** (2005), 65-78.

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

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

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

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

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

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

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

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

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