European Journal of Combinatorics 30 (2009) 30–38

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

On imprimitive multiplicity-free permutation groups the degree of which is the product of two distinct primes

Mitsugu Hirasaka

Department of Mathematics, College of Science, Pusan National University, Kumjung, Busan 609-735, Republic of Korea

ARTICLE INFO

Article history:
Received 9 September 2007
Accepted 2 March 2008
Available online 16 April 2008

ABSTRACT

Let $\mathcal{PQ}$ denote the set of $n \in \mathbb{N}$ such that n is a product of two primes with $\gcd(n, \varphi(n)) = 1$ where φ is the Euler function. In this article we aim to find $n \in \mathcal{PQ}$ such that any imprimitive permutation group of degree n is multiplicity-free. Let $\mathcal{R}$ denote the set of such integers in $\mathcal{PQ}$. Our main theorem shows that there are at most finitely many Fermat primes if and only if $|\mathcal{PQ} - \mathcal{R}|$ is finite, whose proof is based on the classification of finite simple groups.

1. Introduction

Let $\mathcal{PQ}$ denote the set of $n \in \mathbb{N}$ such that n is a product of two primes with $\gcd(n, \varphi(n)) = 1$ where φ is the Euler function.

We say that a group action is *multiplicity-free* if its permutation character is multiplicity-free. Until now there are many results to find multiplicity-free actions of a given group (see [9] for example). In this article we aim to find $n \in \mathcal{PQ}$ such that any imprimitive permutation group of degree n is multiplicity-free. Let $\mathcal{R}$ denote the set of such integers in $\mathcal{PQ}$. Then our main theorem shows that there are at most finitely many Fermat primes if and only if $|\mathcal{PQ} - \mathcal{R}|$ is finite as follows:

Theorem 1.1. *We have* $\mathcal{PQ} - \mathcal{R} = \{pq \mid q \equiv 2 \bmod p\}$ *where q is a Fermat prime and p is a prime.*

Notice that only $\{3, 5, 17, 257, 65\,537\}$ are the known Fermat primes and it is conjectured that there are at most finitely many Fermat primes. This implies that any imprimitive permutation group of degree $n \in \mathcal{PQ}$ is multiplicity-free except very restricted degrees as in Theorem 1.1. Remark that, if $\{3, 5, 17, 257, 65\,537\}$ is the set of Fermat primes, then $|\mathcal{PQ} - \mathcal{R}| = 10$.

E-mail address: hirasaka@pusan.ac.kr.

0195-6698/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2008.03.001

We have to mention that our main theorem owes much to the classification of transitive permutation groups of prime degree by W. Feit (see Theorem 3.3), which is based on the classification of finite simple groups.

We shall mention what makes us focus on $\mathcal{PQ}$.

Let G denote a transitive permutation group of a finite set Ω. Then G acts on $\Omega \times \Omega$ by $(\alpha, \beta)^x := (\alpha^x, \beta^x)$ where $(\alpha, \beta) \in \Omega \times \Omega$ and $x \in G$. It is well known that the set of orbits under the action of G on $\Omega \times \Omega$ forms an association scheme called *Schurian*, and it is commutative if and only if the permutation character associated with the action of G on Ω is multiplicity-free (see [1,16] or [17] for the basic concepts of association schemes).

Originally, our motivation is derived from commutativity of association schemes. In [8] it is proved that each association scheme of prime order is commutative. In [5,6], partial results for commutativity of association schemes of prime square order are obtained. So, it is natural to ask about commutativity of association schemes of order in $\mathcal{PQ}$, while it is still open that each association schemes of prime square order is commutative.

Let $\mathcal{MF}$ denote the set of $n \in \mathbb{N}$ such that any transitive permutation group of degree n is multiplicity-free.

Remark that each prime or prime square is a member of $\mathcal{MF}$ and the order of a nonabelian group is not a member of $\mathcal{MF}$. In this sense $\mathcal{PQ}$ seems to have nontrivial cases in determining members of $\mathcal{MF}$.

Here we notice that

$$\mathcal{PQ} \cap \mathcal{MF} \subseteq \mathcal{R} \subseteq \mathcal{PQ},$$

and both inclusions are proper by the following examples:

Example 1.1. If $r + 1$ is a Fermat prime, then $PSL_2(r) \simeq SL_2(r)$ has a subgroup H isomorphic to $AGL_1(r)$, and H has a subgroup L of index p where p is an odd prime divisor of $r - 1$. The action of $PSL_2(r)$ on the right cosets of L induces an imprimitive permutation group of degree $p(r + 1)$ which is not multiplicity-free (see Lemma 3.6 for the proof). The graph obtained by an orbital under this action is known as Marušič–Scapellato graphs (see [13]).

Example 1.2. According to [2] $PSL_2(13)$ has a subgroup of index 91, and the induced action is primitive but not multiplicity-free. In [12] the primitive permutation groups of square-free degree are classified, and in [14] the vertex-primitive graphs of order a product of two distinct primes are classified. Thus, it remains to enumerate multiplicity-free permutation groups among the classification list.

As a combinatorial interest derived from this topic we refer [10] to introduce a special case of *generalized conference* matrices.

Let $m, n \in \mathbb{N}$. We call an $n \times n$ matrix M a *generalized conference matrix* over $C_m := \{z \in \mathbb{C} \mid z^m = 1\}$ if all diagonal entries of M are zero, each nondiagonal entry of M belongs to C_m and $M\bar{M}^t$ is a scalar of the identity matrix where $\bar{M}^t$ is the transposed and conjugate matrix of M.

Let M denote a symmetric generalized conference matrix of degree n over C_p where p is a prime. Then we can construct imprimitive association scheme of order pn (see Propositions 4.3 and 4.4), which generalizes the association schemes derived from the group action given in Example 1.1.

In Section 2 we prepare notation and basic results, in Section 3 we prove our main theorem. In Section 4 we will show a way of the above construction.

2. Preliminaries

We use the same notation on permutation groups as in [3] and that on association schemes as in [17].

Let G denote a group acting on a nonempty finite set Ω. For each $g \in G$ we denote by g^Ω the permutation of Ω mapping $\alpha \in \Omega$ to α^g. We set $G^\Omega := \{g^\Omega \mid g \in G\}$ and $G_{(\Omega)} := \{g \in G \mid g^\Omega = id_\Omega\}$ so that they are the image and kernel of the action, respectively.