Discrete Mathematics 309 (2009) 3006–3012

Contents lists available at ScienceDirect

Discrete Mathematics

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

Common circulant homogeneous factorisations of the complete digraph[☆]

Cheryl Praeger[a], Cai Heng Li[a], Linda Stringer[a,b,*]

[a] *School of Mathematics and Statistics, The University of Western Australia, Crawley 6009 WA, Australia*

[b] *Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, United Kingdom*

ARTICLE INFO

Article history:
Received 23 November 2006
Received in revised form 26 July 2008
Accepted 28 July 2008
Available online 30 August 2008

Keywords:
Homogeneous factorisation
Circulant
Complete digraph
Complete graph

ABSTRACT

In this paper we determine the positive integers n and k for which there exists a homogeneous factorisation of a complete digraph on n vertices with k 'common circulant' factors. This means a partition of the arc set of the complete digraph K_n into k circulant factor digraphs, such that a cyclic group of order n acts regularly on the vertices of each factor digraph whilst preserving the edges, and in addition, an overgroup of this permutes the factor digraphs transitively amongst themselves. This determination generalises a previous result for self-complementary circulants.

1. Introduction

In this paper we determine the positive integers n and k for which there exists a homogeneous factorisation of a complete digraph on n vertices with k 'common circulant' factors, that is, there is a cyclic group of order n that acts regularly on the vertices and preserves the edges of each factor. This determination, in Theorem 2, generalises for homogeneous factorisations a result of Fronček, Rosa, and Širáň in [3] about self-complementary circulants, in much the same way that the result [7, Theorem 1.1] (which motivated our work) generalised a theorem of Muzychuk [11] characterising orders of self-complementary vertex-transitive graphs. In Theorem 3 we draw from these results a characterisation of integers n for which there exists a homogeneous factorisation of a complete digraph on n vertices, and those integers n for which there exists a common circulant such factorisation. We also determine the analogous results for the complete (undirected) graph. In the remainder of this introductory section we introduce the concepts of homogeneous factorisation and common circulant homogeneous factorisation, and state our main results.

1.1. Homogeneous factorisations

A *digraph* or *directed graph*, $\Gamma = (V\Gamma, A\Gamma)$ consists of a set of *vertices* $V\Gamma$, and a set of *arcs* $A\Gamma$, where an arc is an ordered pair of distinct vertices. Thus $A\Gamma \subseteq V\Gamma^{(2)} = \{(\alpha, \beta) \mid \alpha, \beta \in V\Gamma, \alpha \neq \beta\}$. A *factorisation* of a digraph Γ is a partition $\mathcal{P} = \{P_1, \dots, P_k\}$ of the arc set with at least two parts. This gives rise to *factor digraphs*, $\Gamma_i = (V\Gamma, P_i)$. A *homogeneous factorisation* of a digraph Γ on vertex set Ω, is a factorisation $\mathcal{P}$ such that the following conditions hold.

1. There exist transitive permutation groups M and G with $M < G \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(\Omega)$.

[☆] This paper forms part of an Australian Research Council Discovery Grant project, and a major part of the MSc project of the third author.

[*] Corresponding author at: Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, United Kingdom. Tel.: +44 01784 443093; fax: +44 01784 430766.

E-mail addresses: praeger@maths.uwa.edu.au (C. Praeger), li@maths.uwa.edu.au (C.H. Li), l.c.stringer@rhul.ac.uk (L. Stringer).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.07.034

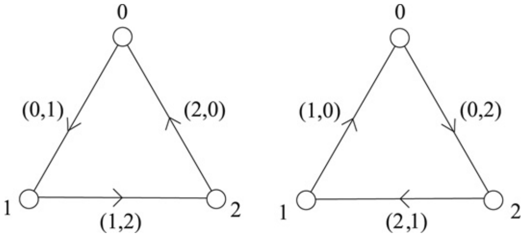

Fig. 1. The factor digraphs of a homogeneous factorisation of degree 3 and index 2.

2. $\mathcal{P}$ is G-invariant (that is, for each $P \in \mathcal{P}$, the image $P^g := \{(\alpha^g, \beta^g) : (\alpha, \beta) \in P\}$ is also a part of $\mathcal{P}$), and the induced action of G on $\mathcal{P}$ is transitive.
3. The group M fixes setwise each part of $\mathcal{P}$ (or equivalently, the induced action of M on $\mathcal{P}$ is trivial).

Since M fixes P_i setwise we have $M \le \mathrm{Aut}(\Gamma_i)$ for each i, and thus the factor digraphs Γ_i are M-vertex transitive. Also because G acts transitively on $\mathcal{P}$, the factor digraphs are pairwise isomorphic. A homogeneous factorisation can be denoted by a quadruple, $(M, G, \Gamma, \mathcal{P})$. The *complete digraph*, K_n, is a digraph with n vertices and $A\Gamma = V\Gamma^{(2)}$. In this paper we consider factorisations of the complete digraph, and we denote the homogeneous factorisation by $(M, G, \Omega, \mathcal{P})$, where Ω is the vertex set of the complete digraph under consideration.

The *degree* of a homogeneous factorisation $(M, G, \Gamma, \mathcal{P})$ is the number of vertices of the digraph Γ. The number of parts in $\mathcal{P}$ is called the *index* of the factorisation. In particular, in a homogeneous factorisation of a complete digraph of degree n and index 2, the factor digraphs are vertex-transitive self-complementary digraphs on n vertices. A homogeneous factorisation of a complete digraph of degree n and index k is a generalisation of this. We illustrate this concept, as we will do for subsequent concepts, with the smallest example.

Example 1. See Fig. 1. Let $\Omega = \{0, 1, 2\}$, $P_1 = \{(0, 1), (1, 2), (2, 0)\}$, $P_2 = \{(0, 2), (2, 1), (1, 0)\}$, $M = \langle(012)\rangle$, $G = \langle M, (12)\rangle$, and $\mathcal{P} = \{P_1, P_2\}$. Then $(M, G, \Omega, \mathcal{P})$ is a homogeneous factorisation of degree 3 and index 2.

A factorisation is *symmetric* if for each factor P_i, we have $(\alpha, \beta) \in P_i$ if and only if $(\beta, \alpha) \in P_i$. A digraph Γ is *undirected*, or simply a *graph* when $(\alpha, \beta) \in A\Gamma$ if and only if $(\beta, \alpha) \in A\Gamma$. Then the arcs (α, β) and (β, α) can be considered as an unordered pair $\{\alpha, \beta\}$, called an *edge*. Thus in a symmetric factorisation, the factor digraphs are considered undirected and this is equivalent to a factorisation of the edge set of a graph.

Remark 1. A homogeneous factorisation of the complete digraph corresponds to a transitive orbital decomposition or k-TOD, as described by Li and Praeger in [7]. They give many results about k-TODs which can be translated into the language of homogeneous factorisations. One key result is the following, which is used in our proofs below. If there exists a homogeneous factorisation of degree n and index k, then by [7, Lemma 2.5] we have that $n \equiv 1 \pmod{k}$. If there exists a symmetric homogeneous factorisation of degree n and index k, then by [7, Lemma 2.5] we have that $n \equiv 1 \pmod{2k}$. Note that Fig. 1 is not symmetric, and the degree and index satisfy the first condition, that is $3 \equiv 1 \pmod{2}$, but by the second condition there is no symmetric homogeneous factorisation of degree 3.

1.2. Cyclic homogeneous factorisations

If $(M, G, \Omega, \mathcal{P})$ is a symmetric homogeneous factorisation of degree n and index 2, with $\mathcal{P} = \{P_1, P_2\}$, then $G^{\mathcal{P}} \cong \mathbb{Z}_2$ and $\Gamma_i := (\Omega, P_i)$, for $i = 1, 2$, are a pair of vertex-transitive, self-complementary (undirected) graphs on n vertices. In 1998 Muzychuk [11] proved that such a factorisation exists if and only if the following condition $\mathrm{Hom}(n, 4)$ holds, where n_r denotes the r-part of n, for a prime r dividing n, namely the highest power of r dividing n.

$$\mathrm{Hom}(n, 4): \quad \forall \text{ primes } r \text{ dividing } n,\ n_r \equiv 1 \pmod{4}.$$

To prove his result, Muzychuk devised a technique of reducing the self-complementary graphs Γ_i to a set of so-called Sylow subgraphs, which were also vertex-transitive and self-complementary, and had a prime power number of vertices. In 2003 Li and Praeger extended this result for *cyclic homogeneous factorisations* of arbitrary index k, that is, for homogeneous factorisations $(M, G, \Omega, \mathcal{P})$ of index k such that the induced group $G^{\mathcal{P}} \cong \mathbb{Z}_k$. Their result involved the following extension of Muzychuk's condition, namely, for a positive integer k,

$$\mathrm{Hom}(n, k): \quad \forall \text{ primes } r \text{ dividing } n,\ n_r \equiv 1 \pmod{k}.$$

The following theorem is their result stated in the language of homogeneous factorisations.

Theorem 1 (*[7, Theorem 1.1]*). *Let n and k be integers such that $n \ge 3$ and $k \ge 2$.*

1. *There exists a cyclic homogeneous factorisation of degree n and index k if and only if* $\mathrm{Hom}(n, k)$ *holds.*

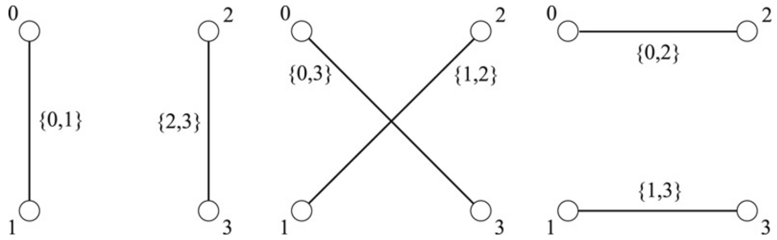

Fig. 2. The factor graphs of a symmetric homogeneous factorisation of degree 4 and index 3.

2. *There exists a symmetric cyclic homogeneous factorisation of degree n and index k if and only if* $\mathrm{Hom}(n/n_2, 2k)$ *holds with* $n_2 \equiv 1 \pmod{k}$.

Note that, if n is odd, then the condition in the symmetric case is equivalent to the condition that $\mathrm{Hom}(n, 2k)$ holds. Muzychuk's result corresponds to the symmetric case with index 2. Example 2 gives the smallest symmetric cyclic homogeneous factorisation.

Example 2. See Fig. 2. Let $\Omega = \{0, 1, 2, 3\}$, $P_1 = \{\{0, 1\}, \{2, 3\}\}$, $P_2 = \{\{0, 3\}, \{1, 2\}\}$, $P_3 = \{\{0, 2\}, \{1, 3\}\}$, $M = \{(01)(23), (02)(13), (03)(12)\}$, $G = \langle M, (123)\rangle \cong A_4$, and $\mathcal{P} = \{P_1, P_2, P_3\}$. Then $G^{\mathcal{P}} \cong \mathbb{Z}_3$ and $(M, G, \Omega, \mathcal{P})$ is a symmetric cyclic homogeneous factorisation of degree 4 and index 3.

Remark 2. We thank Aleksandar Ivić for his interest in these results. In particular he asked about the density of positive integers n for which these kinds of homogeneous factorisations exist: for example, the density of integers n for which there exists a symmetric cyclic homogeneous factorisation of K_n. Determining the density seems a difficult problem. However Ivić has kindly informed us of the solution when the index is restricted to $k = 2$.

For a positive real number x, let $M(x)$ denote the cardinality of the set of positive integers $n \le x$ such that there exists a vertex-transitive self-complementary graph of order n, that is to say, $\mathrm{Hom}(n, 4)$ holds. Ivić has computed the asymptotics of $M(x)$. In particular he has shown [4] that

$$M(x) = \frac{cx}{(\log x)^{1/2}} + O\left(\frac{x}{(\log x)^{3/2}}\right)$$

where $c = 0.5403868\ldots$.

1.3. *Common circulant homogeneous factorisations*

For a group X and a subset $S \subseteq X \setminus \{1_X\}$, the *Cayley digraph of X with respect to S* is the digraph which has vertex set X such that (x, y) is an arc if and only if $yx^{-1} \in S$. A permutation group X on a set Ω is said to be *regular* if X is transitive and only the identity element fixes a point. Moreover, if X is a regular permutation group on Ω, then we may identify the point set Ω with X in such a way that the permutation group X acts by right multiplication. We use $\widehat{X}$ to denote this subgroup of $\mathrm{Sym}(X)$, that is $\widehat{X} = \{\widehat{x} \mid x \in X, \text{ where } \widehat{x} : y \mapsto yx \text{ for all } y \in X\}$. In particular, every Cayley digraph of a group X admits $\widehat{X}$ as a regular group of automorphisms. Conversely for a graph Γ, if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup X, then $\Gamma \cong \mathrm{Cay}(X, S)$, where $S := \{x | (\alpha, \alpha^x) \in A\Gamma\}$ for any $\alpha \in V\Gamma$. A graph Γ is called a *circulant* if $\mathrm{Aut}(\Gamma)$ contains a cyclic regular subgroup, or equivalently if Γ is a Cayley graph of a cyclic group. A Cayley graph $\mathrm{Cay}(M, S)$ is undirected when the connection set S has the property $S = S^{-1}$.

We call a homogeneous factorisation $(M, G, \Omega, \mathcal{P})$ *common circulant* if M contains a cyclic regular subgroup. Thus in a common circulant homogeneous factorisation, all of the factor digraphs Γ_i are circulants relative to the same cyclic regular subgroup, X say where $X \le M$, and we may identify the vertex set with X in such a way that each Γ_i is a Cayley digraph of X.

We now give an example of a common circulant homogeneous factorisation, where the factors are circulants relative to $\mathbb{Z}_n$. We use additive notation for $\mathbb{Z}_n$ (so $\widehat{\mathbb{Z}_n} = \{\widehat{x} \mid x \in \mathbb{Z}_n, \text{ where } \widehat{x} : y \mapsto y + x \text{ for all } y \in \mathbb{Z}_n\}$). For a subset $S \subseteq \mathbb{Z}_n$ and an integer m, let $m \cdot S := \{m \cdot s \mid s \in S\}$. If $\gcd(m, n) = 1$, then multiplication by m is an automorphism of $\mathbb{Z}_n$, which we denote by σ_m.

Example 3. We make use of the element σ_7 of $\mathrm{Aut}(\mathbb{Z}_{25})$ which is of order 4 and acts semi-regularly on $\mathbb{Z}_{25} \setminus \{0\}$. Let $S = \{1, 2, 3, 5, 6, 9\}$ (then S consists of one element of each orbit of σ_7 on $\mathbb{Z}_{25} \setminus \{0\}$). For $i \in \{1, 2, 3, 4\}$, let $S_i = S^{\sigma_7^{i-1}}$, so $S_1 = S$, $S_2 = 7 \cdot S = \{7, 10, 13, 14, 17, 21\}$ etc. For each i, let $\Gamma_i = \mathrm{Cay}(\mathbb{Z}_{25}, S_i)$, and let $P_i = A\Gamma_i$. Let $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$. Then $(\widehat{\mathbb{Z}_{25}}, \langle \widehat{\mathbb{Z}_{25}}, \sigma_7\rangle, \mathbb{Z}_{25}, \mathcal{P})$ is a common circulant cyclic homogeneous factorisation of degree 25 and index 4.

The main result of this paper is the following theorem, which involves the condition below. It is interesting to compare the conditions of Theorems 1 and 2.

$$\mathrm{CommonCirc}(n,k): \quad \forall \text{ primes } r \text{ dividing } n,\ r \equiv 1 \pmod{k}.$$

Theorem 2. *Let n and k be integers such that $n \geq 3$ and $k \geq 2$.*

1. *There exists a common circulant homogeneous factorisation of degree n and index k if and only if* $\mathrm{CommonCirc}(n,k)$ *holds.*
2. *There exists a symmetric common circulant homogeneous factorisation of degree n and index k if and only if* $\mathrm{CommonCirc}(n,2k)$ *holds.*

In 1996 Fronček, Rosa and Širáň [3] proved that there exists a self-complementary (undirected) circulant of order n if and only if $\mathrm{CommonCirc}(n,4)$ holds, and in 1999 Alspach, Morris and Vilfred [1] gave a different proof of the same result. A self-complementary (undirected) circulant corresponds to a symmetric common circulant homogeneous factorisation of the complete digraph of index 2. Therefore Theorem 2 generalises Fronček, Rosa and Širáň's result.

Remark 3. (a) The factorisation in Example 1 is a common circulant cyclic factorisation, because $\langle(012)\rangle = M = \mathrm{Aut}(\Gamma_1) = \mathrm{Aut}(\Gamma_2)$. The degree and the index satisfy the relation above, i.e. $\mathrm{CommonCirc}(3,2)$ holds.

(b) Example 2 is not a common circulant factorisation, even though the factor graphs are circulants: although $\langle(0213)\rangle < \mathrm{Aut}(\Gamma_1)$, $\langle(0132)\rangle < \mathrm{Aut}(\Gamma_2)$, and $\langle(0123)\rangle < \mathrm{Aut}(\Gamma_3)$, there are no groups $X \leq M \leq G \leq \mathrm{Sym}(\Omega)$ such that X is a cyclic regular subgroup of M, and $(M,G,\Omega,\mathcal{P})$ is a homogeneous factorisation. Note that the degree $4 = 2^2$ and the index 3 fail to satisfy the condition in Theorem 2. In fact it is easy to verify that there are no common circulant factorisations of degree 4.

1.4. Commentary on homogeneous factorisations

Theorems 1 and 2 provide necessary and sufficient conditions on the pair (n,k) for existence of cyclic, or common circulant homogeneous factorisations, respectively, of degree n and index k. In Theorem 3 we make a different comparison by determining when homogeneous factorisations (which are not necessarily cyclic) of degree n exist, for some unspecified index.

Theorem 3. *Let n be an integer such that $n \geq 3$.*

1. *There exists a homogeneous factorisation of degree n if and only if* $\mathrm{Hom}(n,p)$ *holds for some prime p; and there exists a common circulant homogeneous factorisation of degree n if and only if n is odd.*
2. *There exists a symmetric homogeneous factorisation of degree n if and only if* $\mathrm{Hom}(n/n_2,2p)$ *holds for some prime p with* $n_2 \equiv 1 \pmod{p}$*; there exists a symmetric common circulant factorisation of degree n if and only if* $\mathrm{CommonCirc}(n,2p)$ *holds for some prime p.*

Before giving a proof, we first state a theorem of Li and Praeger in the language of homogeneous factorisations.

Theorem 4 (*[7, Theorem 3.6]*). *Let $(M,G,\Omega,\mathcal{P})$ be a homogeneous factorisation of degree n and index k, with M normal in G. Then there exists a cyclic homogeneous factorisation $(M,H,\Omega,\mathcal{Q})$ of degree n and index p for some prime divisor p of k, and some partition $\mathcal{Q}$ refined by $\mathcal{P}$, where $H = \langle M,\tau\rangle$ with $\tau \in G_\omega \setminus M_\omega$ for some $\omega \in \Omega$.*

Note that for a homogeneous factorisation $(M,G,\Omega,\mathcal{P})$ of degree n and index k, if K is the kernel of the action of G on $\mathcal{P}$, then $(K,G,\Omega,\mathcal{P})$ is also a homogeneous factorisation of degree n and index k. Thus, replacing M with the normal closure of M in G if necessary, we may assume that $M \lhd G$. If the original factorisation is cyclic or common circulant, these properties are preserved under such a replacement of M.

Proof of Theorem 3. (1) First suppose that there exists a homogeneous factorisation $(M,G,\Omega,\mathcal{P})$ of degree n and index k, for some k. Then by Theorem 4, there exists a cyclic homogeneous factorisation $(M,H,\Omega,\mathcal{Q})$ of degree n and index p for some prime p dividing k, and hence, by Theorem 1, $\mathrm{Hom}(n,p)$ holds. The converse statement follows immediately from Theorem 1. Next suppose that $(M,G,\Omega,\mathcal{P})$ is common circulant, that is, M contains a cyclic regular subgroup. Then $(M,H,\Omega,\mathcal{Q})$ is also common circulant, and hence $\mathrm{CommonCirc}(n,p)$ holds by Theorem 2. This means that for any prime divisor r of n, $r \equiv 1 \pmod{p}$, so $r \geq 3$ and n is odd. Conversely, if n is odd, then $\mathrm{CommonCirc}(n,2)$ holds and, again by Theorem 2, there exists a common circulant factorisation of degree n and index 2.

(2) Suppose that the homogeneous factorisation $(M,G,\Omega,\mathcal{P})$ above is symmetric (but not necessarily common circulant). Then, the cyclic homogeneous factorisation $(M,H,\Omega,\mathcal{Q})$ of degree n and index p is also symmetric since the partition $\mathcal{Q}$ of Theorem 4 is refined by $\mathcal{P}$. Thus by Theorem 1, $\mathrm{Hom}(n/n_2,2p)$ holds with $n_2 \equiv 1 \pmod{p}$. The converse statement follows immediately from Theorem 1. Finally suppose that $(M,G,\Omega,\mathcal{P})$ is symmetric and common circulant. Then $(M,H,\Omega,\mathcal{Q})$ is also symmetric and common circulant of index p, and hence $\mathrm{CommonCirc}(n,2p)$ holds by Theorem 2. The converse statement follows immediately from Theorem 2. □

1.5. Comment on the proof of Theorem 2 and Zibin's conjecture

A proof of the necessity conditions of Theorem 2 was given in [13], and two proofs were also given there for the necessity conditions of a slightly weaker version of Theorem 2 (concerning common circulant homogeneous factorisations which are also cyclic). Only the first of these three proofs is included in this paper. It uses 'Zibin's conjecture', which is known to be true, as discussed below. The second proof uses the technique of reducing the factorisation to a common ciruclant factorisation of the same index but on the vertices which comprise a single orbit of a Sylow subgroup of our group G. This is a method of Li and Praeger devised in [7], which is a generalisation of Muzychuk's method which he used for self-complementary vertex-transitive digraphs in [11]. The third proof uses induction, and relies on the classification of finite primitive permutation groups containing a cyclic regular subgroup which was published independently by Li in 2003 [6] and Jones in 2002 [5], and which itself depends on the classification of finite simple groups.

Zibin's conjecture was developed from Ádám's conjecture, which was published in 1967, and was shown to be false in general in 1970.

Conjecture 5 (*Ádám's Conjecture*). *Suppose* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are two isomorphic circulants. Then there exists an element* $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$ *such that* $S^\sigma = T$.

In 1987, Pálfy proposed a corrected form of Ádám's conjecture. He suggested the values of n for which Ádám's conjecture holds (namely, when n is not divisible by 8 or a square of an odd prime). In 1995/1997 Muzychuck proved that Pálfy's formulation was correct [9,10], using group theory and Schur rings. Zibin's conjecture is a similar result, but it holds for all integers n. Let d be a divisor of a positive integer n, and for $S \subseteq \mathbb{Z}_n$ let $S(d) := \{x \in S \mid \gcd(x, n) = d\}$.

Theorem 6 (*Zibin's Conjecture*). *If* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are isomorphic Cayley digraphs, then for each divisor d of n, there exists an element* $m \in \mathbb{Z}_n$*, such that* $\gcd(m, n) = 1$ *and* $m \cdot S(d) = T(d)$.

According to [12], D.K. Zibin is an expert in technical cybernetics, and his conjecture was proposed in 1975 as an empirical observation based on the analysis of results of his computer experiments. Zibin's conjecture was proved in 1999 by Muzychuk, Pöschel and Klin, using Schur rings [12, Theorem 5.1]. Independently (although their paper did not appear until 2002), Dobson and Morris proved Toida's conjecture (which was proposed in 1977 and is the particular case of Zibin's conjecture where $d = 1$) in [2, Corollary 2.7], see also [8, Chapter 3], and then proved in [2, Corollary 2.9] that Toida's conjecture in fact implies Zibin's conjecture. Their proof of Toida's conjecture relies on the classification of finite simple groups.

In the second section of this paper, we give in Section 2.1 a general construction that proves the sufficiency conditions of Theorem 2, and then in Section 2.2 we apply elementary group theory and use Zibin's conjecture to prove the necessity condition.

We give a final example, this time of a common circulant homogeneous factorisation which demonstrates a failure of Ádám's conjecture. In the example, for each distinct pair i, j with $i, j \in \{1, 2, 3\}$, the factor graphs $\mathrm{Cay}(\mathbb{Z}_{49}, S_i)$ and $\mathrm{Cay}(\mathbb{Z}_{49}, S_j)$ are isomorphic circulants, but there is no element of $\mathrm{Aut}(\mathbb{Z}_{49})$ which maps S_i to S_j.

Example 4. We make use of an element σ_{19} of $\mathrm{Aut}(\mathbb{Z}_{49})$ which is of order 6 and acts semi-regularly on $\mathbb{Z}_{49} \setminus \{0\}$. If $x \in Z_{49}$ such that $x \equiv 1 \pmod 7$, then $x^{\sigma_{19}} = 19 \cdot x \equiv 5 \pmod 7$, $x^{\sigma_{19}^2} = 19^2 \cdot x \equiv 4 \pmod 7$, $x^{\sigma_{19}^3} = 19^3 \cdot x \equiv 6 \pmod 7$ and so on. Let $S = \{x \in Z_{49} \mid x \equiv 1 \pmod 7\} = \{1, 8, 15, 22, 29, 36, 43\}$ and let $T = \{7\}$. Define

$$S_1 = S \cup S^{\sigma_{19}} \cup T \cup T^{\sigma_{19}^3},$$
$$S_2 = S^{\sigma_{19}^2} \cup S^{\sigma_{19}^3} \cup T^{\sigma_{19}} \cup T^{\sigma_{19}^4},$$
$$S_3 = S^{\sigma_{19}^4} \cup S^{\sigma_{19}^5} \cup T^{\sigma_{19}^2} \cup T^{\sigma_{19}^5}.$$

Recall the notation given just before Theorem 6. For example $S_1(7) = \{x \in S_1 \mid \gcd(x, 49) = 7\} = \{7, 42\} = T \cup T^{\sigma_{19}^3}$ and $S_2(7) = \{14, 35\}$. Then σ_{19} maps $S_1(7)$ to $S_2(7)$ to $S_3(7)$ and back again to $S_1(7)$. Furthermore σ_{19}^2 maps $S_1(1)$ to $S_2(1)$ to $S_3(1)$ and back again to $S_1(1)$. Now let $\tau \in \mathrm{Sym}(\mathbb{Z}_{49})$ be defined as follows: $\tau : x \mapsto x^{\sigma_{19}}$ if $x \in \mathbb{Z}_{49}(7)$, and $\tau : x \mapsto x^{\sigma_{19}^2}$ if $x \in \mathbb{Z}_{49}(1)$. Then τ maps S_1 to S_2 to S_3 to S_1.

For $i \in \{1, 2, 3\}$, let $\Gamma_i = \mathrm{Cay}(\mathbb{Z}_{49}, S_i)$, and let $P_i = A\Gamma_i$. Let $\mathcal{P} = \{P_1, P_2, P_3\}$. Then $(\widehat{\mathbb{Z}}_{49}, \langle \widehat{\mathbb{Z}}_{49}, \tau \rangle, \mathbb{Z}_{49}, \mathcal{P})$ is a common circulant cyclic homogeneous factorisation of degree 49 and index 3. It is not symmetric as, for example, $(0, 1)$ is an arc of Γ_1 while $(1, 0)$ is an arc of Γ_3.

An automorphism of $\mathbb{Z}_{49}$ is σ_m for some m such that $\gcd(m, 49) = 1$. Suppose that $S_1^{\sigma_m} = S_2$. Since $1 \in S_1$ it follows that $m = 1^{\sigma_m} \in S_2$. Thus $m \equiv 4 \pmod 7$ or $m \equiv 6 \pmod 7$. Also since $7 \in S_1$, then $7^{\sigma_m} \in S_2$. If $m \equiv 4 \pmod 7$ then $7^{\sigma_m} = m \cdot 7 \equiv 28 \pmod{49}$, and if $m \equiv 6 \pmod 7$ then $7^{\sigma_m} = m \cdot 7 \equiv 42 \pmod{49}$. However $28 \in S_3$ and $42 \in S_1$, so there is no automorphism of $\mathbb{Z}_{49}$ which maps S_1 to S_2.

2. Proof of Theorem 2

2.1. Proof of the sufficiency condition

We use Cayley digraphs to give a construction of a common circulant homogeneous factorisation, and thereby provide a proof of Proposition 7, the sufficiency condition of our main result Theorem 2. This construction is from [14], see also [13].

Proposition 7. *Let n and k be integers such that $n \geq 3$ and $k \geq 2$.*

1. *If* $\mathrm{CommonCirc}(n, k)$ *holds then there exists a common circulant homogeneous factorisation of degree n and index k.*
2. *If* $\mathrm{CommonCirc}(n, 2k)$ *holds then there exists a symmetric common circulant homogeneous factorisation of degree n and index k.*

The proof is a direct consequence of the construction given below. This construction can be used to obtain our Example 3, but not Example 4. First we give a brief summary of the theory required. Note that, if $\mathrm{CommonCirc}(n, k)$ holds, then n is odd.

Let $n = r_1^{d_1} \dots r_m^{d_m}$ where the r_i are distinct primes. Then $\mathbb{Z}_n \cong \mathbb{Z}_{r_1^{d_1}} \times \cdots \times \mathbb{Z}_{r_m^{d_m}}$, and so $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{r_1^{d_1}}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}_{r_m^{d_m}})$. Now for positive integers r and d, where r is an odd prime, $\mathrm{Aut}(\mathbb{Z}_{r^d}) \cong \mathbb{Z}_{r^{d-1}(r-1)}$, and $\mathrm{Aut}(\mathbb{Z}_{r^d})$ has a cyclic subgroup of order $r - 1$ which acts semi-regularly on $\mathbb{Z}_{r^d} \setminus \{0\}$. Suppose that $\mathrm{CommonCirc}(n, k)$ holds, and let $s = gcd\,\{r_i - 1 : i = 1, \dots, m\}$. For $i = 1, \dots, m$, let σ_i be a generator for the cyclic subgroup of $\mathrm{Aut}(\mathbb{Z}_{r_i^{d_i}})$ of order $r_i - 1$ which acts semi-regularly on $\mathbb{Z}_{r_i^{d_i}} \setminus \{0\}$. Then $\langle \sigma_i^{(r_i-1)/s} \rangle$ also acts semi-regularly on $\mathbb{Z}_{r_i^{d_i}} \setminus \{0\}$, with orbits of length s. In $\mathrm{Aut}(\mathbb{Z}_n)$, there is therefore an element σ which corresponds to the element $(\sigma_1^{(r_1-1)/s}, \dots, \sigma_m^{(r_m-1)/s})$ of $\mathrm{Aut}(\mathbb{Z}_{r_1^{d_1}}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}_{r_m^{d_m}})$, and such that $\langle \sigma \rangle$ acts semi-regularly on $\mathbb{Z}_n \setminus \{0\}$ with orbits of length s. Our construction uses this element σ.

Construction 8. *Let $n = r_1^{d_1} \dots r_m^{d_m}$, where the r_i are distinct primes, $d_i \geq 1$ and $m \geq 1$, and suppose that* $\mathrm{CommonCirc}(n, k)$ *holds. Let $s = \gcd\{r_i - 1 : i = 1, \dots, m\}$ (note that k divides s). Let σ be an element of* $\mathrm{Aut}(\mathbb{Z}_n)$ *of order s such that $\langle \sigma \rangle$ acts semi-regularly on $\mathbb{Z}_n \setminus \{0\}$. Take S to consist of one representative of each $\langle \sigma \rangle$-orbit on $\mathbb{Z}_n \setminus \{0\}$. Let*

$$S_1 = \{\alpha^{\sigma^{jk}} : \alpha \in S \text{ and } j = 1, \dots, s/k\},$$

and for $l = 2, \dots, k$, let $S_l = S_1^{\sigma^{l-1}}$. Let

$$P_l = \{(\alpha, \beta) : \alpha, \beta \in \mathbb{Z}_n \text{ and } \beta - \alpha \in S_l\},$$

so P_l is the arc set of the digraph $\Gamma_l = \mathrm{Cay}(\mathbb{Z}_n, S_l)$. Let $\mathcal{P} = \{P_1, \dots, P_m\}$. Then $(\widehat{\mathbb{Z}}_n, \langle \widehat{\mathbb{Z}}_n, \sigma \rangle, \mathbb{Z}_n, \mathcal{P})$ is a common circulant homogeneous factorisation of degree n and index k.

It is straightforward to verify the assertions of the last sentence of Construction 8, thus proving part 1 of Proposition 7. Concerning part 2 of Proposition 7, if $\mathrm{CommonCirc}(n, 2k)$ holds, then the factorisation obtained using Construction 8 is symmetric, as we now explain. Recall that a Cayley graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ is undirected when the connection set S has the property $S = -S$ (we are using additive notation for $\mathbb{Z}_n$). If $\mathrm{CommonCirc}(n, 2k)$ holds, then $2k$ divides s, and for each $\alpha \in S_1$, we also have $\alpha^{\sigma^{s/2}} \in S_1$. Now $\alpha^{\sigma^{s/2}} = -\alpha$ because $\langle \sigma \rangle$ acts semi-regularly on $\mathbb{Z}_n \setminus \{0\}$, so $S_1 = -S_1$, and the same is true for $S_2, \dots, S_k$. Therefore if $\mathrm{CommonCirc}(n, 2k)$ holds, the factor graphs are undirected, or equivalently, the factorisation is symmetric.

2.2. Proof of the necessity condition

The following corollary to Zibin's conjecture is used in the proof of Proposition 11.

Corollary 9. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *be isomorphic Cayley digraphs.*

1. *For each divisor d of n, there exists an automorphism σ_m of $\mathbb{Z}_n$ such that $S(d)^{\sigma_m} = T(d)$.*
2. *For each prime divisor r of n, S and T contain an equal number of elements of $\mathbb{Z}_n$ of order r.*

Proof. (1) This follows directly from Theorem 6, since multiplication by such an element m of $\mathbb{Z}_n$ is the automorphism σ_m of $\mathbb{Z}_n$ which maps $1 \mapsto m$.

(2) Now $\mathbb{Z}_n(n/r)$ is the set of elements of $\mathbb{Z}_n$ of order r. Thus $S(n/r)$ and $T(n/r)$ are the sets of elements of S and T respectively of order r. By the above, there exists an automorphism $\sigma_m \in \mathrm{Aut}(\mathbb{Z}_n)$, such that $S(n/r)^{\sigma_m} = T(n/r)$. Since automorphisms are 1–1, we have $|S(n/r)| = |T(n/r)|$, and so S and T contain an equal number of elements of $\mathbb{Z}_n$ of order r. □

Now suppose that $(M, G, \Omega, \mathcal{P})$ is a homogeneous factorisation, and let $X = \langle x \rangle$ be a cyclic regular subgroup of M so (by definition) this factorisation is common circulant. Suppose that $\mathcal{P} = \{P_1, \dots, P_k\}$, so the index of the factorisation is k, and for each i let Γ_i be the factor digraph with arc set P_i. Let $\omega \in \Omega$ and for each $P_i \in \mathcal{P}$ let $P_i(\omega) = \{\alpha \in \Omega : (\omega, \alpha) \in P_i\}$. Finally let $\mathcal{S} = \{S_1, \dots, S_k\}$ where $S_i = \{j : \omega^{x^j} \in P_i(\omega)\}$, and let $\Sigma_i = \mathrm{Cay}(\mathbb{Z}_n, S_i)$.

Lemma 10. *$\mathcal{S}$ is a partition of $\mathbb{Z}_n \setminus \{0\}$, and furthermore $\Gamma_i \cong \Sigma_i$ for each i.*

Proof. Let ψ be the bijection $\psi : \mathbb{Z}_n \to \Omega$ defined by $\psi : j \mapsto \omega^{x^j}$. This is a bijection because X is regular. Then for all i, we have $\psi(S_i) = P_i(\omega)$. Since $\{P_1(\omega), \ldots, P_k(\omega)\}$ partitions $\Omega \setminus \{\omega\}$, it follows that $\{S_1, \ldots, S_k\}$ partitions $\mathbb{Z}_n \setminus \{0\}$.

Now $\mathbb{Z}_n = V\Sigma_i$ and $\Omega = V\Gamma_i$, and note that $(\alpha, \beta) \in A\Sigma_i$ if and only if $\beta - \alpha \in S_i$ if and only if $\omega^{x^{\beta-\alpha}} \in P_i(\omega)$. Moreover $\omega^{x^{\beta-\alpha}} \in P_i(\omega)$ if and only if $(\omega, \omega^{x^{\beta-\alpha}}) \in P_i$ if and only if $(\omega, \omega^{x^{\beta-\alpha}})^{x^\alpha} \in P_i = A\Gamma_i$. Now $(\omega, \omega^{x^{\beta-\alpha}})^{x^\alpha} = (\omega^{x^\alpha}, \omega^{x^\beta}) = (\psi(\alpha), \psi(\beta))$. Thus we have shown that $(\alpha, \beta) \in A\Sigma_i$ if and only if $(\psi(\alpha), \psi(\beta)) \in A\Gamma_i$, and so $\Gamma_i \cong \Sigma_i$. □

Now the necessity assertions of Theorem 2 follow as an application of Corollary 9 and Lemma 10. Recall that the condition CommonCirc(n, k) means that for all prime divisors r of n, we have $r \equiv 1 \pmod{k}$.

Proposition 11. *Let n and k be integers such that $n \geq 3$ and $k \geq 2$.*

1. *If there exists a common circulant homogeneous factorisation of degree n and index k, then* CommonCirc(n, k) *holds.*
2. *If there exists a symmetric common circulant homogeneous factorisation of degree n and index k, then* CommonCirc$(n, 2k)$ *holds.*

Proof. (1) Consider the common circulant homogeneous factorisation $(M, G, \Omega, \mathcal{P})$ and the associated terms specified above. Since the Γ_i are pairwise isomorphic, it follows that the Σ_i are pairwise isomorphic. Let r be a prime divisor of n. Then by Corollary 9, all the S_i contain an equal number of elements of $\mathbb{Z}_n$ of order r. Now there are precisely $r - 1$ such elements, namely $\mathbb{Z}_n(n/r) = \{n/r, 2n/r, \ldots, (r-1)n/r\}$, and $S_i(n/r) = \mathbb{Z}_n(n/r) \cap S_i$. Thus $|S_i(n/r)| = (r-1)/k$, so k divides $r - 1$, and $r \equiv 1 \pmod{k}$.

(2) If the factorisation is symmetric, the factor digraphs are undirected, so $S_i = -S_i$ for $i = 1, \ldots, k$, and since an element and its inverse have the same order, we have $S_i(n/r) = -S_i(n/r)$. Also r must be odd since $k \geq 2$ and $r \equiv 1 \pmod{k}$ implies that $r > 2$. This means that each element x of $S_i(n/r)$ is distinct from its inverse $-x$, and hence since $S_i(n/r) = -S_i(n/r)$, $|S_i(n/r)|$ is even. Then since $|S_i(n/r)| = (r-1)/k$, it follows that $r \equiv 1 \pmod{2k}$. □

Acknowledgments

The authors thank the anonymous reviewers for their comments on an earlier version of this paper. In particular we thank the second reviewer for pointing out a misunderstanding about the results in one of the references, and for the suggestion to re-organize our results. We also thank Joy Morris for making available to us a copy of her Ph.D. thesis, and for the correspondence regarding the proof of Toida's Conjecture.

References

[1] Brian Alspach, Joy Morris, V. Vilfred, Self-complementary circulant graphs, Ars Combin. 53 (1999) 187–191.

[2] Edward Dobson, Joy Morris, Toida's conjecture is true, Electron. J. Combin. 9 (1) (2002) Research Paper 35, 14 pp. (electronic).

[3] Dalibor Frončeк, Alexander Rosa, Jozef Širáň, The existence of selfcomplementary circulant graphs, European J. Combin. 17 (7) (1996) 625–628.

[4] Aleksandar Ivić, Private communication, 2006.

[5] Gareth A. Jones, Cyclic regular subgroups of primitive permutation groups, J. Group Theory 5 (4) (2002) 403–407.

[6] Cai Heng Li, The finite primitive permutation groups containing an abelian regular subgroup, Proc. London Math. Soc. (3) 87 (3) (2003) 725–747.

[7] Cai Heng Li, Cheryl E. Praeger, On partitioning the orbitals of a transitive permutation group, Trans. Amer. Math. Soc. 355 (2) (2003) 637–653 (electronic).

[8] Joy Morris, Isomorphisms of Cayley graphs, Ph.D. Thesis, Simon Fraser University, Department of Mathematics and Statistics, November 1999.

[9] Mikhail Muzychuk, Ádám's conjecture is true in the square-free case, J. Combin. Theory Ser. A 72 (1) (1995) 118–134.

[10] Mikhail Muzychuk, On Ádám's conjecture for circulant graphs, Discrete Math. 176 (1–3) (1997) 285–298.

[11] Mikhail Muzychuk, On Sylow subgraphs of vertex-transitive self-complementary graphs, Bull. London Math. Soc. 31 (5) (1999) 531–533.

[12] Mikhail Muzychuk, Mikhail Klin, Reinhard Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, in: Codes and Association Schemes (Piscataway, NJ, 1999), in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc, Providence, RI, 2001, pp. 241–264.

[13] Linda Stringer, Homogeneous factorisations of complete digraphs, Masters dissertation, University of Western Australia, School of Mathematics and Statisitcs, July 2004.

[14] Luke Tredwell, Circulant factorisations of complete graphs, Honours dissertation, University of Western Australia, School of Mathematics and Statisitcs, April 2002.