Orthogonal decompositions of complete digraphs

SVEN HARTMANN
FB Mathematik, Universität Rostock, 18051 Rostock, Germany

June 30, 1998

Abstract

A family $\mathcal{G}$ of isomorphic copies of a given digraph $\vec{\mathfrak{G}}$ is said to be an orthogonal decomposition of the complete digraph $\vec{\mathfrak{D}}_n$ by $\vec{\mathfrak{G}}$, if every arc of $\vec{\mathfrak{D}}_n$ belongs to exactly two members of $\mathcal{G}$ and the union of any two different elements from $\mathcal{G}$ contains precisely one pair of reverse arcs.
Given a digraph $\vec{\mathfrak{H}}$, an $\vec{\mathfrak{H}}$-family $m\vec{\mathfrak{H}}$ is the vertex-disjoint union of m copies of $\vec{\mathfrak{H}}$. In this paper, we consider orthogonal decompositions by $\vec{\mathfrak{H}}$-families. Our objective is to prove the existence of such an orthogonal decomposition whenever certain necessary conditions hold and m is sufficiently large.

1 Introduction

A collection $\mathcal{G}$ of subdigraphs of a digraph $\vec{\mathfrak{D}}$ is said to be a *decomposition* of $\vec{\mathfrak{D}}$ iff every arc of $\vec{\mathfrak{D}}$ belongs to exactly one member of $\mathcal{G}$. Throughout, the subdigraphs in $\mathcal{G}$ are called the *pages* of the decomposition. If, in addition, all pages in $\mathcal{G}$ are isomorphic to a given digraph $\vec{\mathfrak{G}}$, we speak of a *decomposition by* $\vec{\mathfrak{G}}$.

For any positive integer n, let $\vec{\mathfrak{D}}_n$ denote the complete (symmetric) digraph on n vertices. A decomposition $\mathcal{G}$ of $\vec{\mathfrak{D}}_n$ is said to be *orthogonal* if the union of any two distinct pages in $\mathcal{G}$ contains exactly one digon, i.e. a copy of $\vec{\mathfrak{D}}_2$.

Decomposition problems of graphs have received much attention during the last two decades. Orthogonal decompositions were studied first by Hering and Rosenfeld [10], who asked for an orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by a directed $(n-1)$-cycle. Even though this problem is far from being solved, it gave rise to a considerable number of results concerning orthogonal decompositions by special digraphs. Several papers deal with the undirected analogue of the problem, i.e. with orthogonal double covers of complete graphs. For a survey on this topic see Alspach, Heinrich and Liu [1].

For a digraph $\vec{\mathfrak{H}}$, let $m\vec{\mathfrak{H}}$ denote the vertex-disjoint union of m copies of $\vec{\mathfrak{H}}$ and call it an $\vec{\mathfrak{H}}$-*family* of size m. In this paper, we concentrate on orthogonal decompositions by $\vec{\mathfrak{H}}$-families. In the sequel, let $\vec{\mathfrak{H}}$ always denote a simple digraph, i.e. without multiple arcs, loops and digons.

Let the vertex set of $\vec{\mathfrak{D}}_n$ be $V = \{0, 1, \ldots, n-1\}$. A page $\vec{\mathfrak{G}}_v$ is said to be *idempotent* iff it contains vertex v as a singleton (or does not contain vertex v at all). An orthogonal decomposition shall be called *idempotent* iff all its pages are idempotent.

When considering keys and antikeys in databases, Demetrovics and Katona [6] asked for idempotent orthogonal decompositons of $\vec{\mathfrak{D}}_n$ by directed 3-cycle families. A first, partial answer to this question was given by Demetrovics, Füredi and Katona [5]. Rausche [12] proved that there is no such decomposition of $\vec{\mathfrak{D}}_{10}$. Finally, the problem was completely solved by Bennett and Wu [2] and, independently, by Ganter and Gronau [7] who proved the existence of an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by a directed 3-cycle family iff $n \equiv 1 \bmod 3$ and $n \neq 10$.

More recently, Granville, Gronau and Mullin [8] proved that for every $k \geq 3$ there exists an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by a directed k-cycle family whenever the necessary condition $n \equiv 1 \bmod k$ holds and n is sufficiently large. This question was asked in the undirected case by Hering [9].

Our objective is to generalize the latter result to arbitrary digraph families. We shall prove the existence of an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by an $\vec{\mathfrak{H}}$-family for almost all n whenever certain necessary conditions hold. These preconditions are given by the following lemma.

Lemma 1. *Let $\vec{\mathfrak{H}}$ be a simple digraph with $v(\vec{\mathfrak{H}})$ vertices and $e(\vec{\mathfrak{H}})$ arcs. If there exists an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by an $\vec{\mathfrak{H}}$-family then $v(\vec{\mathfrak{H}}) \leq e(\vec{\mathfrak{H}})$ and $n \equiv 1 \bmod e(\vec{\mathfrak{H}})$ hold.*

Proof. Assume, there exists an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by an $\vec{\mathfrak{H}}$-family $\vec{\mathfrak{G}} = m\vec{\mathfrak{H}}$ of size m. For the numbers of vertices and arcs in $\vec{\mathfrak{D}}_n$ we obtain

$$v(\vec{\mathfrak{D}}_n) = n \geq v(\vec{\mathfrak{G}}) + 1 = m\ v(\vec{\mathfrak{H}}) + 1$$

and

$$e(\vec{\mathfrak{D}}_n) = n(n-1) = n\ e(\vec{\mathfrak{G}}) = nm\ e(\vec{\mathfrak{H}}),$$

respectively. This implies $e(\vec{\mathfrak{H}}) \geq v(\vec{\mathfrak{H}})$ as well as $n - 1 \equiv 0 \bmod e(\vec{\mathfrak{H}})$. □

The difference $e(\vec{\mathfrak{H}}) - v(\vec{\mathfrak{H}})$ is usually called the *cyclomatic number* of the digraph $\vec{\mathfrak{H}}$. Thus we are looking for orthogonal decompositions by $\vec{\mathfrak{H}}$-families where $\vec{\mathfrak{H}}$ has non-negative cyclomatic number.

2 Preliminaries

In this section we shall assemble some terminology and basic results which will be required in the sequel. Throughout, let q denote a prime power, and let a and b be positive integers such that $q = ab + 1$ holds. Consider $V = \{0, \ldots, q-1\}$ to be the finite field $GF(q)$ of order q. Let Γ denote its cyclic multiplicative group containing all non-zero elements of $GF(q)$, and let T be its unique subgroup of cardinality a and index b. If w denotes a generator of Γ, then T is clearly generated by w^b.

A *character* on Γ is a map χ from Γ to the complex numbers satisfying $|\chi(x)| = 1$ and $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in \Gamma$. The characters on Γ form again a cyclic group of order $q-1$, the dual group Γ^* of Γ.

It will be convenient to extend the usual definition of a character χ on Γ by putting

$$\chi(0) = \begin{cases} 1 & \text{if } \chi = \chi^0, \\ 0 & \text{otherwise,} \end{cases}$$

where χ^0 is the principal character with $\chi(x) = 1$ for all $x \in \Gamma$.

Let T^* be the unique subgroup of index a and cardinality b in Γ^*. If ψ denotes a generator of Γ^* then T^* is clearly generated by ψ^a. The interplay between the characters in T^* and the elements in T is given by the following well-known equality (see e.g. [14]):

$$\sum_{\chi \in T^*} \chi(x) = \sum_{j=0}^{b-1} \psi^{aj}(x) = \begin{cases} b & \text{if } x \in T, \\ 1 & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Let f be a polynomial of positive degree d over $GF(q)$, and let E be an extension field of $GF(q)$. Then f is said to *split* in E iff f can be written as a product of linear factors over E, i.e. iff there exist elements $x_1, \ldots, x_d \in E$ such that

$$f(x) = z(x - x_1) \cdots (x - x_d),$$

where z is the leading coefficient of f. The values $x_1, \ldots, x_d$ are called the *roots* of f. Note that there is a (up to isomorphism) unique smallest extension field containing all roots of f, the *splitting field* of f. For more detailed information on polynomials and splitting fields, we refer to [13].

We are interested in sums of the form $\sum_{x \in GF(q)} \chi(f(x))$, where χ is a fixed character and f a fixed polynomial over $GF(q)$. The problem of evaluating character sums is known to be difficult in general. One usually has to be satisfied with estimates for the absolute value of such sums. We shall make use of the following result [15]. (The interested reader may consult e.g. [13, 14].)

Theorem 2 (Weil). *Let f be a polynomial of positive degree over $GF(q)$ such that f is not the b-th power of a polynomial over $GF(q)$. Let r be the number of pairwise* *distinct roots of f in a splitting field of f. Then*

$$|\sum_{x\in GF(q)} \psi^a(f(x))| \le (r-1)q^{1/2}$$

holds, where ψ denotes a generator of the dual group Γ^*.

If X and Y are two subsets of Γ, their product XY is defined as the set $\{xy \in \Gamma : x \in X \text{ and } y \in Y\}$. If $X = \{x\}$ we shall briefly write xY instead of $\{x\}Y$. Moreover, let X^{-1} denote the set $\{x^{-1} : x \in X\}$ of all inverses of the elements in X.

Let w be a generator of Γ. We now consider the *cosets* $T_i = w^i T$ of Γ modulo T, where i is some integer. T_i and T_j denote the same coset whenever $i \equiv j \bmod b$ holds. The cosets themselves form again a group Γ/T known as the factor group of Γ (with respect to T). The order of Γ/T is just $(q-1)/|T| = b$.

We continue with a somewhat technical result that forms the foundation of what follows.

Lemma 3. *Let b be a positive integer and r, s be non-negative integers. There is a constant $q_3 = q_3(b, r, s)$ such that for all prime powers $q \ge q_3$ with $q \equiv 1 \bmod b$, for all r-sets $U \subseteq GF(q)$, for all s-sets $Z \subseteq GF(q)$ and for all maps $\theta : U \to \Gamma/T$ there exists an element $x \in GF(q)$ satisfying*

$$x \notin Z, \tag{2}$$
$$x - u \in \theta(u) \tag{3}$$

for every $u \in U$.

Proof. The claim is trivial when $r = 0$ holds. Conversely, let r be positive. An element $x \in GF(q)$ lies in coset T_i modulo T iff $w^{-i}x$ lies in T, where w denotes as above a generator of Γ. For every integer i and for every element $x \in GF(q)$, put

$$S_i(x) = \frac{1}{b}\sum_{\chi\in T^*} \chi(w^{-i}x) = \begin{cases} 1 & \text{if } x \in T_i, \\ \frac{1}{b} & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

The idea is to use such sums to construct an expression which has value 1 whenever (3) holds and becomes sufficiently small otherwise. For the sake of simplicity, we define a function $\iota : U \to \{0, \ldots, b-1\}$ given by $\theta(u) = T_{\iota(u)}$ for every $u \in U$.

Next, we put

$$P(x) = \prod_{u\in U} S_{\iota(u)}(x-u).$$

Some consequences of (4) may be noted immediately. We have $P(x) = 1$ iff (3) holds. Moreover, $P(x)$ is positive iff $x - u \in \theta(u) \cup \{0\}$ holds for every $u \in U$. This implies $0 < P(x) < 1$ iff we have $x - u \in \theta(u) \cup \{0\}$ for every $u \in U$, and x lies in U. Hence there are at most r elements x satisfying $0 < P(x) < 1$. We emphasize that in this case we actually have $0 < P(x) \leq 1/b$.

Finally, we put

$$Q = \sum_{x \in GF(q)} P(x).$$

Then $Q > r/b$ implies the existence of an element $x \in GF(q)$ with $P(x) = 1$, i.e. (3) holds. The existence of an appropriate x satisfying (2) and (3) will follow if $Q > r/b + s$.

We shall show that Q becomes larger than $r/b + s$ if q is sufficiently large. To begin with, we find that

$$\begin{aligned} Q &= \frac{1}{b^r} \sum_{x \in GF(q)} \prod_{u \in U} \sum_{\chi \in T^*} \chi(w^{-\iota(u)}(x-u)) \\ &= \frac{1}{b^r} \sum_{x \in GF(q)} \prod_{u \in U} \sum_{j=0}^{b-1} \psi^{aj}(w^{-\iota(u)}(x-u)), \end{aligned}$$

where ψ denotes as above a generator of Γ^*.

Let M denote the set of all r-tuples $\underline{j} = (j_u : u \in U) \in \{0, \ldots, b-1\}^r$. On expanding and recombining Q, we obtain

$$\begin{aligned} Q &= \frac{1}{b^r} \sum_{\underline{j} \in M} \sum_{x \in GF(q)} \prod_{u \in U} \psi^{aj_u}(w^{-\iota(u)}(x-u)) \\ &= \frac{1}{b^r} \sum_{\underline{j} \in M} \sum_{x \in GF(q)} \prod_{u \in U} \psi^{a}(w^{-j_u\iota(u)}(x-u)^{j_u}) \\ &= \frac{1}{b^r} \sum_{\underline{j} \in M} \sum_{x \in GF(q)} \psi^{a}(w^{-\sum_{u \in U} j_u \iota(u)} \prod_{u \in U}(x-u)^{j_u}). \end{aligned}$$

For every tuple $\underline{j} \in M$, put

$$z_{\underline{j}} = w^{-\sum_{u \in U} j_u \iota(u)},$$

and let

$$f_{\underline{j}}(x) = \prod_{u \in U}(x-u)^{j_u}$$

be a polynomial of degree $\sum_{u\in U} j_u$ over $GF(q)$.

If $\underline{j}$ is the tuple with all zero-entries, simply denoted by $\underline{o}$, then $z_{\underline{o}} = w^0 = 1$ and $f_{\underline{o}}$ is the constant polynomial of value 1 for all $x \in GF(q)$. Hence, we obtain

$$\sum_{x\in GF(q)} \psi^a(z_{\underline{o}} f_{\underline{o}}(x)) = \sum_{x\in GF(q)} \psi^a(1) = q. \tag{5}$$

Conversely, let $\underline{j}$ be different from $\underline{o}$. The roots of $f_{\underline{j}}$ are just the elements $u \in U$ which satisfy $j_u > 0$. Hence, $f_{\underline{j}}$ has at most r distinct roots. Since all components j_u in $\underline{j}$ are smaller than b, and at least one of them is positive, $f_{\underline{j}}$ is not the b-th power of a polynomial over $GF(q)$. Applying Weil's theorem, we obtain

$$|\sum_{x\in GF(q)} \psi^a(z_{\underline{j}} f_{\underline{j}}(x))| = |\psi^a(z_{\underline{j}})||\sum_{x\in GF(q)} \psi^a(f_{\underline{j}}(x))| \le (r-1)q^{1/2} \tag{6}$$

for every $\underline{j} \neq \underline{o}$.

Combining (5) and (6) we obtain

$$\begin{aligned}
Q - \frac{1}{b^r}\sum_{x\in GF(q)} \psi^a(z_{\underline{o}} f_{\underline{o}}(x)) &= \frac{1}{b^r}\sum_{\underline{j}\neq\underline{o}}\sum_{x\in GF(q)} \psi^a(z_{\underline{j}} f_{\underline{j}}(x)) \\
|Q - \frac{1}{b^r}\sum_{x\in GF(q)} \psi^a(z_{\underline{o}} f_{\underline{o}}(x))| &\le \frac{1}{b^r}\sum_{\underline{j}\neq\underline{o}}|\sum_{x\in GF(q)} \psi^a(z_{\underline{j}} f_{\underline{j}}(x))| \\
|Q - \frac{1}{b^r}q| &\le \frac{1}{b^r}(b^r-1)(r-1)q^{1/2} \\
|Q - \frac{1}{b^r}q| &\le (r-1)q^{1/2}
\end{aligned}$$

and thus

$$Q \ge \frac{1}{b^r}q - (r-1)q^{1/2},$$

which tends to infinity when $q \to \infty$.

So x can be chosen satisfying (2) and (3) if q is large enough. This concludes the proof. A straightforward, but tendious calculation shows that $q_3 = q_3(b,r,s) = b^{2r}(r+s)^2 + 1$ will be a lower bound for q to ensure the existence of an appropriate $x \in GF(q)$. $\square$

In the sequel, let Ω_k denote the set $\{1,\ldots,k\}$. A *choice* over $GF(q)$ is a map $C : \Omega_k^2 \to \Gamma/T$ assigning a coset modulo T to each pair (i,j) of integers $i,j \in \Omega_k$. With the help of our Lemma 3 it is easy to verify that there exists a k-tuple $\underline{x} =$

$(x_1, \ldots, x_k)$ of elements in Γ satisfying $x_j - x_i \in C(i,j)$ for every pair $i, j \in \Omega_k$ with $i < j$ whenever q is large enough. The latter result is originally due to Wilson [16, 18] and was used to prove the asymptotic existence of pairwise balanced designs [19]. For details, we refer to [3]. Our objective is to prove several generalizations of Wilson's result.

Lemma 4. *Let b, k be positive integers. There is a constant $q_4 = q_4(b,k)$ such that for all odd prime powers $q \geq q_4$ with $q \equiv 1 \bmod b$ and for all maps $C : \Omega_k^2 \to \Gamma/T$ there exists a k-tuple $\underline{x}$ of elements from $GF(q)$ satisfying*

$$\begin{aligned} -x_i + x_j &\in C(i,j) && \text{if } i < j, \\ x_j &\in C(i,j) && \text{if } i = j, \\ x_i + x_j &\in C(i,j) && \text{if } i > j \end{aligned} \tag{7}$$

for all pairs $(i,j) \in \Omega_k^2$.

Proof. We shall proceed by induction on k. For $k = 1$ the claim is trivially true: just choose x_1 from the coset $C(1,1)$ which is non-empty for $q \geq 2$.

Assume, the statement is true for $k-1$, and we shall prove it for k, now. Let $\underline{x} = (x_1, \ldots, x_{k-1})$ be a $(k-1)$-tuple satisfying (7) for each pair $(i,j) \in \Omega_{k-1}^2$.

It remains to find an element $x_k \in C(k,k)$ with $x_k - x_i \in C(i,k)$ and $x_k + x_i \in C(k,i)$ for every $i \in \Omega_{k-1}$. It turns out that Lemma 3 ensures the existence of such an element x_k when putting $Z = \emptyset$ and $U = \{0, x_1, \ldots, x_{k-1}, -x_1, \ldots, -x_{k-1}\}$. Note that the elements 0, x_i $(i \in \Omega_{k-1})$ and $-x_i$ $(i \in \Omega_{k-1})$ are pairwise distinct by virtue of the induction hypothesis and since q is odd.

We must now define a map θ on U by

$$\theta(u) = \begin{cases} C(k,k) & \text{if } u = 0, \\ C(i,k) & \text{if } u = x_i, \\ C(k,i) & \text{if } u = -x_i \end{cases}$$

for every element $u \in U$. Hence, we are looking for an element $x_k \in GF(q)$ such that $x_k - u \in \theta(u)$ holds for every $u \in U$. By Lemma 3, such an element exists whenever $q \geq q_3(b, 2k-1, 0)$. $\square$

Unfortunately, for even prime powers, the statement of Lemma 3 is usually false since $y - x = y + x$ holds for all elements $x, y \in GF(q)$ if q is even. However, the following weaker result holds.

Lemma 5. *Let b, k be positive integers. There is a constant $q_5 = q_5(b, k)$ such that for all even prime powers $q \geq q_5$ with $q \equiv 1 \bmod b$ and for all maps $C : \Omega_k^2 \to \Gamma/T$ there exists a k-tuple $\underline{x}$ of elements from $GF(q)$ satisfying*

$$\begin{aligned} x_i + x_j = -x_i + x_j &\in C(i,j) && \text{if } i < j, \\ x_j &\in C(i,j) && \text{if } i = j \end{aligned}$$

for all pairs $(i,j) \in \Omega_k^2$.

Proof. The proof works analogously to the proof of Lemma 4. This time we obtain $q_5 = q_3(b, k, 0)$. □

We now consider choices C over $GF(q)$ assigning a coset modulo T to every 4-tuple $(g, h, i, h) \in \Omega_k^4$. Applying Lemma 3 we shall verify the following claim which holds for both, even and odd prime powers.

Lemma 6. *Let b, k be positive integers. There is a constant $q_6 = q_6(b, k)$ such that for all prime powers $q \geq q_6$ with $q \equiv 1 \bmod b$ and for all maps $C : \Omega_k^4 \to \Gamma/T$ there exists a k-tuple $\underline{x}$ with elements from $GF(q)$ satisfying*

$$\begin{aligned} x_j &\in C(g,h,i,j) && \text{if} \quad g = h = i = j, \\ -x_i + x_j &\in C(g,h,i,j) && \text{if} \quad g = h = i < j, \\ -x_g x_h + x_i x_j &\in C(g,h,i,j) && \text{if} \quad g \leq h < i < j \\ & && \quad \text{or} \quad g < i < h < j \quad \text{or} \quad i < g \leq h < j \end{aligned} \tag{8}$$

for all 4-tuples $(g,h,i,j) \in \Omega_k^4$.

Proof. Again we shall proceed by induction on k. However, we shall prove the slightly stronger statement that there is a k-tuple $\underline{x}$ satisfying not only (8) but also

$$x_g x_h x_i \neq x_{g'} x_{h'} x_{i'} \tag{9}$$

whenever two multisets $\{g, h, i\}$ and $\{g', h', i'\}$ over Ω_k are distinct.

When $k = 1$ the claim trivially holds: just choose x_1 in the coset $C(1,1,1,1)$ which is non-empty for $q \geq 2$. Assume, the statement is true for $k - 1$, and we shall prove it for k, now.

Let $\underline{x} = (x_1, \ldots, x_{k-1})$ be a $(k-1)$-tuple satisfying (8) for each 4-tuple $(g,h,i,j) \in \Omega_{k-1}^4$ as well as our additional property (9). We are interested in an element $x_k \in C(k,k,k,k)$ with $x_k - x_i \in C(i,i,i,k)$ for every $i \in \Omega_{k-1}$ and $x_k - x_g x_h x_i^{-1} \in C(g,h,i,k)C(i,i,i,i)^{-1}$ for every 3-tuple $(g,h,i) \in \Omega_{k-1}^+$, where

$$\Omega_{k-1}^+ = \{(g,h,i) \in \Omega_{k-1}^3 : g \leq h < i \text{ or } g < i < h \text{ or } i < g \leq h\}.$$

In order to apply Lemma 3, we put

$$U = \{0, x_1, \ldots, x_{k-1}\} \cup \{x_g x_h x_i^{-1} : (g,h,i) \in \Omega_{k-1}^+\},$$

and

$$Z = XXXX^{-1}X^{-1} \cup \{z : z^2 \in XXXX^{-1}\} \cup \{z : z^3 \in XXX\},$$

where X denotes the set $\{x_1, \ldots, x_{k-1}\}$ containing the components of the $(k-1)$-tuple $\underline{x}$. On U we define a map $\theta : U \to \Gamma/T$ by

$$\theta(u) = \begin{cases} C(k,k,k,k) & \text{if } u = 0, \\ C(j,j,j,k) & \text{if } u = x_j, \\ C(g,h,i,k)C(i,i,i,i)^{-1} & \text{if } u = x_g x_h x_i^{-1} \end{cases}$$

for every integer $j \in \Omega_{k-1}$ and every 3-tuple $(g,h,i) \in \Omega_{k-1}^+$.

In general, this definition will only be correct if the elements 0, x_j $(j \in \Omega_{k-1})$ and $x_g x_h x_i^{-1}$ $((g,h,i) \in \Omega_{k-1}^+)$ are pairwise distinct.

It is readily verified that the elements 0 and x_j $(j \in \Omega_{k-1})$ are pairwise distinct by the induction hypothesis. For the same reason, all the elements $x_g x_h x_i^{-1}$ are different from 0.

Next suppose, there are two distinct 3-tuples (g,h,i) and (g',h',i') in Ω_{k-1}^+ such that $x_g x_h x_i^{-1} = x_{g'} x_{h'} x_{i'}^{-1}$ holds. This implies $x_g x_h x_{i'} = x_{g'} x_{h'} x_i$, and by virtue of (9) for $k-1$, the multisets $\{g,h,i'\}$ and $\{g',h',i\}$ are equal. Since $i \neq g,h$, we obtain $i = i'$. Moreover, $g \leq h$ and $g' \leq h'$ imply $g = g'$ as well as $h = h'$. Clearly, this gives a contradiction.

Finally suppose, there is an integer $j \in \Omega_{k-1}$ and a 3-tuple $(g,h,i) \in \Omega_{k-1}^+$ such that $x_j = x_g x_h x_i^{-1}$ holds. This implies $x_i x_j = x_g x_h$, and again by the induction hypothesis (9), the multisets $\{i,j\}$ and $\{g,h\}$ are equal. But $i \neq g,h$, which gives a contradiction.

By Lemma 3, there exists an element $x_k \in GF(q)$ satisfying $x_k - u \in \theta(u)$ for every $u \in U$ and $x_k \notin Z$ if $q \geq q_3(b, k^3, 6k^5)$. Note, that $|U| \leq k^3$ and $|Z| \leq 6k^5$ hold.

To satisfy our additional property (9) we have to ensure $x_g x_h x_i \neq x_{g'} x_{h'} x_{i'}$ whenever the multisets $\{g,h,i\}$ and $\{g',h',i'\}$ over Ω_k are distinct. If k is neither in $\{g,h,i\}$ nor in $\{g',h',i'\}$, then the claim follows from the induction hypothesis. Conversely assume, there are two distinct multisets $\{g,h,i\}$ and $\{g',h',i'\}$ over Ω such that $x_g x_h x_i = x_{g'} x_{h'} x_{i'}$ holds and k lies in $\{g,h,i,g',h',i'\}$. Thus we obtain $x_k \in XXXX^{-1}X^{-1}$ or $x_k^2 \in XXXX^{-1}$ or $x_k^3 \in XXX$. But such a relation contradicts $x_k \notin Z$. This concludes the proof. $\square$

The preceding lemmas require large prime powers q satisfying the additional condition $q \equiv 1 \bmod b$ for a given integer b. The existence of such prime powers is ensured by Dirichlet's well-known theorem on primes in arithmetic progressions (cf. [11]). We record this result for future reference.

Theorem 7 (Dirichlet). *Let p_7, b, r be positive integers with g.c.d.$\{b, r\} = 1$. There exists a prime $p \geq p_7$ such that $p \equiv r \bmod b$ holds.*

By a further investigation we may render the following slightly modified existence result on primes in arithmetic progressions.

Lemma 8. *Let p_8, b, r be positive integers with g.c.d.$\{2b, r\} = 1$. There exist two primes p, q with $q > p \geq p_8$ such that $p \equiv q \equiv r \bmod b$ and g.c.d.$\{p(p-r), q(q-r)\} = 2b$ hold.*

Proof. By Dirichlet's theorem there is a prime $p \geq p_8$ with $p \equiv 4b+r \bmod 2b(2b+r)$, say $p = 2b(2b+r)\lambda + 4b + r$ for some positive integer λ. Put $\mu = (2b+r)\lambda + 2$, such that $p = 2b\mu + r$ holds. Again by Dirichlet's theorem there is a prime $q > p$ with $q \equiv 2b + r \bmod 2b\mu p$, say $q = 2b\mu p\nu + 2b + r$ for some positive integer ν. Clearly, $p \equiv q \equiv r \bmod b$ holds. Moreover, we have $g.c.d.\{p(p-r), q(q-r)\} = g.c.d.\{p(p-r), q-r\} = g.c.d.\{2b\mu p, 2b\mu p\nu + 2b\} = 2b\; g.c.d.\{\mu p, \mu p\nu + 1\} = 2b$. $\square$

3 Main constructions

For a given digraph $\vec{\mathfrak{H}}$, let $\mathcal{I}_{\vec{\mathfrak{H}}}$ denote the set of all integers n such that $\vec{\mathfrak{D}}_n$ admits an idempotent orthogonal decomposition by an $\vec{\mathfrak{H}}$-family. Our ultimative aim in this section is to investigate the occurency of prime powers in $\mathcal{I}_{\vec{\mathfrak{H}}}$. In order to study orthogonal decompositions of complete digraphs $\vec{\mathfrak{D}}_q$ where q is a prime power, we shall exploit the concepts presented in Section 2.

It is advantageous to distinguish several cases. To begin with, we consider odd prime powers q satisfying the additional property that $(q-1)/e(\vec{\mathfrak{H}})$ is even.

Lemma 9. *Let $\vec{\mathfrak{H}}$ be a simple digraph with non-negative cyclomatic number. There exists a constant $q_9 = q_9(\vec{\mathfrak{H}})$ such that every odd prime power $q \geq q_9$ with $q \equiv 1 \bmod 2e(\vec{\mathfrak{H}})$ lies in $\mathcal{I}_{\vec{\mathfrak{H}}}$.*

Proof. Put $k = v(\vec{\mathfrak{H}})$ and $b = e(\vec{\mathfrak{H}})$. Consider $V = \{0, \ldots, q-1\}$ to be the finite field $GF(q)$ of order $q = ab + 1$. Throughout, we shall use the terminology introduced in Section 2. In particular, let Γ be the multiplicative group of $GF(q)$, and T its unique subgroup of cardinality a and index b. When w denotes a generator of Γ, then the cosets modulo T are given by $T_i = w^i T$.

Let $W = \{1, \ldots, k\}$ and $B = \{a_l : l = 1, \ldots, b\}$ be the vertex set and arc set of $\vec{\mathfrak{H}}$, respectively. On W^2 we define a map $C : W^2 \to \Gamma/T$ by

$$C(i,j) = \begin{cases} T_{j-1} & \text{if } i = j \in W, \\ T_l & \text{if } (i,j) = a_l \in B \text{ or } (j,i) = a_l \in B, \\ T_0 & \text{otherwise.} \end{cases}$$

Put $q_9 = q_4(b,k)$ and let $q \geq q_9$. Applying Lemma 4 we find a k-tuple $\underline{x}$ satisfying $x_j \in T_{j-1}$ for all vertices j in $\vec{\mathfrak{H}}$, and $x_j - x_i \in T_l$ as well as $x_j + x_i \in T_l$ for all arcs $a_l = (i,j) \in B$. It is worth mentioning that both, the differences $x_j - x_i$ and the sums $x_i + x_j$ taken over all arcs (i,j) in $\vec{\mathfrak{H}}$ form a system of representatives of the cosets modulo T.

For every $v \in V$ and for every $t \in T$, we construct a digraph $\vec{\mathfrak{H}}_v(t)$ as the isomorphic image of $\vec{\mathfrak{H}}$ under the map $j \to tx_j + v$ for all vertices j in $\vec{\mathfrak{H}}$.

First, we shall show that for every fixed $v \in V$ the digraphs $\vec{\mathfrak{H}}_v(t)$ with $t \in T$ are pairwise vertex-disjoint. Assume, there are distinct elements t and t' in T such that the digraphs $\vec{\mathfrak{H}}_v(t)$ and $\vec{\mathfrak{H}}_v(t')$ share a vertex z. Then there are two vertices j and j' in $\vec{\mathfrak{H}}$ such that $z = tx_j + v = t'x_{j'} + v$ holds. This implies $tx_j = t'x_{j'}$. So x_j and $x_{j'}$ lie in the same coset modulo T. Due to our choice of C, we obtain $j = j'$ and consequently $t = t'$, which gives a contradiction. Hence, for fixed $v \in V$ the digraphs $\vec{\mathfrak{H}}_v(t)$, $t \in T$, form an $\vec{\mathfrak{H}}$-family $a\vec{\mathfrak{H}}$ which will be denoted by $\vec{\mathfrak{G}}_v$. It should be mentioned that $\vec{\mathfrak{G}}_v$ has exactly $e(\vec{\mathfrak{G}}_v) = ae(\vec{\mathfrak{H}}) = q - 1$ arcs.

Secondly, we point out that $\vec{\mathfrak{G}}_v$ is idempotent for every $v \in V$. Assume, v is a vertex in $\vec{\mathfrak{G}}_v$. This implies the existence of a vertex j in $\vec{\mathfrak{H}}$ satisfying $tx_j + v = v$ for some element $t \in T$. However, this contradicts $x_j \neq 0$ for all j in $\vec{\mathfrak{H}}$. Thus $\vec{\mathfrak{G}}_v$ is idempotent.

Next, we shall check that the digraphs $\vec{\mathfrak{G}}_v$, $v \in V$, form a decomposition $\mathcal{G}$ of $\vec{\mathfrak{D}}_q$. Let $\mathcal{G}$ denote the collection of all digraphs $\vec{\mathfrak{G}}_v$, $v \in V$. Since each of the q digraphs in $\mathcal{G}$ contains exactly $q-1$ arcs, it suffices to show that every arc of $\vec{\mathfrak{D}}_q$ belongs to at least one of the digraphs $\vec{\mathfrak{G}}_v$.

Let (y,z) be an arbitrary arc in $\vec{\mathfrak{D}}_q$. In $\vec{\mathfrak{H}}$ we find exactly one arc (i,j) such that the difference $x_j - x_i$ lies in the same coset modulo T as the difference $z - y$. Put $t = (z-y)(x_j - x_i)^{-1}$, and $v = y - tx_i = z - tx_j$. Clearly, t is an element of T, and v lies in V. It is now easy to see that the digraph $\vec{\mathfrak{H}}_v(t)$ contains the arc (y,z), and so does the page $\vec{\mathfrak{G}}_v$. We conclude that every arc of $\vec{\mathfrak{D}}_q$ lies in at least one page of $\mathcal{G}$, and consequently, $\mathcal{G}$ forms a decomposition of the complete digraph $\vec{\mathfrak{D}}_q$.

It still remains to prove that $\mathcal{G}$ is orthogonal. Let $\vec{\mathfrak{G}}_v$ and $\vec{\mathfrak{G}}_w$ be two distinct pages of $\mathcal{G}$. There is exactly one arc (i,j) in $\vec{\mathfrak{H}}$ such that the sum $x_i + x_j$ lies in the same coset modulo T as the difference $w - v$. Put $t = (w-v)(x_i + x_j)^{-1}$, which belongs to T. Further, put $y = tx_i + v$ and $z = tx_j + v$. Evidently, $\vec{\mathfrak{G}}_v$ contains the arc (y,z). On the other hand, $y = -tx_j + w$ and $z = -tx_i + w$ hold. It is noteworthy that the field element -1 lies in T since $|T|$ is even. So with t also $-t$ is in T. Hence the arc (z,y) belongs to the page $\vec{\mathfrak{G}}_w$. We obtain that the union of any two pages in $\mathcal{G}$ contains a digon. But there are exactly $q(q-1)/2$ different pairs of pages in $\mathcal{G}$, and $\vec{\mathfrak{D}}_q$ contains just $q(q-1)/2$ digons. It turns out that every pair of distinct pages has precisely one digon in its union. This concludes the proof. $\square$

We continue our study with odd primes q where $(q-1)/e(\vec{\mathfrak{H}})$ happens to be odd. Unfortunately, this case needs a slightly stronger argument. At this point it is convenient to introduce some basic facts on decompositions of graphs and digraphs into stars which will be used later on.

For any positive integer m, let $\mathfrak{S}_{m+1}$ denote the (undirected) m-star, i.e. the complete bipartite graph $\mathfrak{K}_{1,m}$ with m edges and $m+1$ vertices. For $m \geq 2$, it is customary to call the vertex of degree m in $\mathfrak{S}_{m+1}$ the centre of the star.

Lemma 10. *Every simple graph $\mathfrak{H}$ admits a decomposition into copies of $2\mathfrak{S}_2$ and at most one star, or a decomposition into copies of $2\mathfrak{S}_2$ and a triangle.*

Proof. We use induction on the number of edges in $\mathfrak{H}$. If $\mathfrak{H}$ has only one edge or less, than the claim is trivially true. Suppose, the statement holds for all simple graphs with at most $b-1$ edges. We have to verify that it remains true for every simple graph $\mathfrak{H}$ with b edges.

First assume, $\mathfrak{H}$ contains two vertex-disjoint edges. Together, they form a copy of $2\mathfrak{S}_2$. Let $\mathfrak{H}'$ be the graph obtained from $\mathfrak{H}$ by deleting these two edges. By the induction hypothesis, $\mathfrak{H}'$ admits an appropriate decomposition, and so $\mathfrak{H}$ does.

Conversely assume, any two edges in $\mathfrak{H}$ share a vertex. Then $\mathfrak{H}$ is star or a triangle. But then the claim trivially holds. $\square$

From $\mathfrak{S}_{m+1}$ we obtain a directed m-star by assigning a direction to every edge in $\mathfrak{S}_{m+1}$. By $\vec{\mathfrak{S}}^d_{m+1}$ we shall denote the directed m-star whose centre has indegree d and, consequently, outdegree $m-d$. When $m=1$, there exists (up to isomorphism) only one directed 1-star which will be denoted by $\vec{\mathfrak{S}}_2$.

The argument of Lemma 10 applies also to decompositions of digraphs. Here, we shall only state a slightly refined result for digraphs with an even number of arcs.

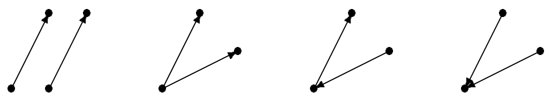

Figure 1: The digraphs $2\vec{\mathfrak{S}}_2$, $\vec{\mathfrak{S}}_3^0$, $\vec{\mathfrak{S}}_3^1$ and $\vec{\mathfrak{S}}_3^2$.

Lemma 11. *Every simple digraph $\vec{\mathfrak{H}}$ with an even number of arcs admits a decomposition into copies of $2\vec{\mathfrak{S}}_2$, of $\vec{\mathfrak{S}}_3^0$, of $\vec{\mathfrak{S}}_3^2$ and at most one copy of $\vec{\mathfrak{S}}_3^1$, such that all copies of $\vec{\mathfrak{S}}_3^0$, $\vec{\mathfrak{S}}_3^1$ and $\vec{\mathfrak{S}}_3^2$ in this decomposition have the same centre.*

Proof. By Lemma 10 the digraph $\vec{\mathfrak{H}}$ admits a decomposition into copies of $2\vec{\mathfrak{S}}_2$ and at most one directed star. Suppose, this star is a copy of $\vec{\mathfrak{S}}_{m+1}^d$ with centre z. Note that m is even by assumption.

If d is even too, $\vec{\mathfrak{S}}_{m+1}^d$ admits a decomposition into $d/2$ copies of $\vec{\mathfrak{S}}_3^2$ and $(m-d)/2$ copies of $\vec{\mathfrak{S}}_3^0$. If d is odd, then $\vec{\mathfrak{S}}_{m+1}^d$ admits a decomposition into $(d-1)/2$ copies of $\vec{\mathfrak{S}}_3^2$, $(m-d-1)/2$ copies of $\vec{\mathfrak{S}}_3^0$ and one copy of $\vec{\mathfrak{S}}_3^1$. This concludes the proof. $\square$

We are now in the position to establish a result similar to Lemma 9 for odd prime powers q where $(q-1)/e(\vec{\mathfrak{H}})$ is odd.

Lemma 12. *Let $\vec{\mathfrak{H}}$ be a simple digraph with non-negative cyclomatic number. There exists a constant $q_{12} = q_{12}(\vec{\mathfrak{H}})$ such that every odd prime power $q \geq q_{12}$ with $q \equiv e(\vec{\mathfrak{H}}) + 1 \bmod 2e(\vec{\mathfrak{H}})$ belongs to $\mathcal{I}_{\vec{\mathfrak{H}}}$.*

Proof. When $e(\vec{\mathfrak{H}})$ is odd, it turns out that there is no odd prime power q satisfying the necessary condiditon $q-1 \equiv e(\vec{\mathfrak{H}}) \bmod 2e(\vec{\mathfrak{H}})$. So henceforth, we suppose that $e(\vec{\mathfrak{H}})$ is even.

Put $k = v(\vec{\mathfrak{H}})$ and $b = e(\vec{\mathfrak{H}})$. Again, we consider $V = \{0, \ldots, q-1\}$ to be the finite field $GF(q)$ of order $q = ab+1$. By Lemma 11, the digraph $\vec{\mathfrak{H}}$ is decomposable into subdigraphs $\vec{\mathfrak{F}}_1, \ldots, \vec{\mathfrak{F}}_{b/2}$ such that each of them is a copy of $2\vec{\mathfrak{S}}_1$ or a directed 2-star.

We denote the arcs in subdigraph $\vec{\mathfrak{F}}_l$ ($l = 1, \ldots, b/2$) by a_l and $a_{b/2+l}$. The collection $B = \{a_1, \ldots, a_b\}$ of all these arcs forms the arc set of $\vec{\mathfrak{H}}$.

Let $W = \{1, \ldots, k\}$ be the vertex set of $\vec{\mathfrak{H}}$. Without loss of generality, let 1 denote the common centre of all directed 2-stars among $\vec{\mathfrak{F}}_1, \ldots, \vec{\mathfrak{F}}_{b/2}$. If, in particular, the decomposition of $\vec{\mathfrak{H}}$ contains a digraph isomorphic to $\vec{\mathfrak{S}}_3^1$, its arcs should be $(2,1)$ and $(1,3)$.

Moreover, if either $(2,3)$ or $(3,2)$ occurs as an arc in $\vec{\mathfrak{H}}$, then we may assume that this arc belongs to the subdigraph $\vec{\mathfrak{F}}_{b/2}$. In other words, suppose $a_{b/2} = (3,2)$ or $a_b = (2,3)$ or neither of these pairs is an arc in $\vec{\mathfrak{H}}$.

As usual, let Γ be the multiplicative group of $GF(q)$ with the unique subgroup T of cardinality a and index b. When w denotes a generator of Γ, the cosets modulo T are the sets $T_i = w^i T$. In order to apply Lemma 5 we define a map $C : W^4 \to \Gamma/T$ by

$$C(g,h,i,j) = \begin{cases} T_{j-1} & \text{if } g = h = i = j \in W, \\ T_l & \text{if } g = h = i < j \text{ and } (i,j) = a_l \in B, \\ T_{b/2+l} & \text{if } g = h = i < j \text{ and } (j,i) = a_l \in B, \\ T_0 & \text{otherwise.} \end{cases}$$

Put $q_{12}(\vec{\mathfrak{H}}) = q_6(b,k)$. For prime powers $q \geq q_{12}(\vec{\mathfrak{H}})$, Lemma 6 ensures the existence of a k-tuple $\underline{x}$ satisfying (8).

Next we construct the pages $\vec{\mathfrak{G}}_v$ in the decomposition $\mathcal{G}$ of the complete digraph $\vec{\mathfrak{D}}_q$. Fix $v \in V$ and $t \in T$. The digraph obtained from $\vec{\mathfrak{H}}$ by assigning the vertex $tx_j + v$ to each vertex j in $\vec{\mathfrak{H}}$ will be denoted by $\vec{\mathfrak{H}}_v(t)$. Similarly to Lemma 9, the digraphs $\vec{\mathfrak{H}}_v(t)$, $t \in T$, are pairwise vertex-disjoint for fixed $v \in V$, and do not contain v as a vertex. Thus, the union $\vec{\mathfrak{G}}_v$ of the digraphs $\vec{\mathfrak{H}}_v(t)$, $t \in T$, forms an idempotent $\vec{\mathfrak{H}}$-family $a\vec{\mathfrak{H}}$.

As in Lemma 12 the collection $\mathcal{G} = \{\vec{\mathfrak{G}}_v : v \in V\}$ turns out to be a decomposition of the complete digraph $\vec{\mathfrak{D}}_q$. This is due to the observation that the differences $x_j - x_i$ taken over all the arcs (i,j) in $\vec{\mathfrak{H}}$ form again a system of representatives of the cosets modulo T.

We now consider the question whether $\mathcal{G}$ is orthogonal, too. Let $\vec{\mathfrak{G}}_v$ and $\vec{\mathfrak{G}}_w$ be two distinct pages of $\mathcal{G}$. Let T_m be the coset modulo T containing the difference $w - v$. Since -1 lies in the coset $T_{b/2}$ this implies $v - w \in T_{b/2+m}$. Thus, we may suppose that $0 \leq m < b/2$. Consider the subdigraph $\vec{\mathfrak{F}}_{b/2-m}$ of $\vec{\mathfrak{H}}$ with arcs $a_{b/2-m} = (i,j)$ and $a_{b-m} = (i',j')$. Due to our choice of the map C, we have $x_j - x_i \in T_{b/2-m}$ and $x_{j'} - x_{i'} \in T_{b-m}$. Put

$$t = (w-v)(x_j - x_i)(x_j x_{j'} - x_i x_{i'})^{-1},$$

and

$$t' = (w-v)(x_{j'} - x_{i'})(x_j x_{j'} - x_i x_{i'})^{-1}.$$

These settings are legal as long as $x_j x_{j'}$ differs from $x_i x_{i'}$. This difficulty is overcome when the difference $x_j x_{j'} - x_i x_{i'}$ lies in coset T_0 or $T_{b/2}$ modulo T.

If $x_jx_{j'} - x_ix_{i'} \in T_0$, we obtain $t \in T_mT_{b/2-m}T_0 = T_{b/2}$ and $t' \in T_mT_{b-m}T_0 = T_0$. Thus, the elements $-t$ and t' lie in the subgroup T of Γ. We put $y = t'x_i + v = (-t)x_{j'} + w$ and $z = t'x_j + v = (-t)x_{i'} + w$. Hence the arc (y, z) lies in $\vec{\mathfrak{H}}_v(t')$ and, consequently, in the page $\vec{\mathfrak{G}}_v$ of $\mathcal{G}$. For the same reason the reverse arc (z, y) belongs to $\vec{\mathfrak{H}}_w(-t)$ and therefore to the page $\vec{\mathfrak{G}}_w$.

Conversely, if $x_jx_{j'} - x_ix_{i'} \in T_{b/2}$, this implies $t \in T_mT_{b/2-m}T_{b/2} = T_0$ and $t' \in T_mT_{b-m}T_{b/2} = T_{b/2}$. This time, t and $-t'$ belong to the subgroup T. We put $y = tx_{i'} + v = (-t')x_j + w$ and $z = tx_{j'} + v = (-t')x_i + w$. Again we find (y, z) in the page $\vec{\mathfrak{G}}_v$ as well as (z, y) in the page $\vec{\mathfrak{G}}_w$. This proves that any two distinct pages of $\mathcal{G}$ have at least one digon in their union. As mentioned in the proof of Lemma 9 this suffices to verify that $\mathcal{G}$ is orthogonal.

It remains to check that $x_jx_{j'} - x_ix_{i'}$ actually is in T_0 or $T_{b/2}$. Four cases arise. First, assume the subdigraph $\vec{\mathfrak{F}}_{b/2-m}$ is isomorphic to $2\vec{\mathfrak{S}}_2$. Then the vertices i, i', j, j' are pairwise distinct. Due to our choice of the map C, this implies $x_jx_{j'} - x_ix_{i'} \in T_0$ or $x_ix_{i'} - x_jx_{j'} \in T_0$ depending on whether $\max\{i, i', j, j'\}$ is in $\{j, j'\}$ or not. However, the latter relation may be rewritten as $x_jx_{j'} - x_ix_{i'} \in T_{b/2}$.

Secondly, assume $\vec{\mathfrak{F}}_{b/2-m}$ is isomorphic to $\vec{\mathfrak{S}}_3^0$. We immediately obtain $i = i' = 1$ and $j \neq j'$. This gives us $x_jx_{j'} - x_ix_{i'} = x_jx_{j'} - x_1x_1 \in T_0$.

Next, let $\vec{\mathfrak{F}}_{b/2-m}$ be isomorphic to $\vec{\mathfrak{S}}_3^2$. In this case we find $j = j' = 1$ and $i \neq i'$. This implies $x_ix_{i'} - x_1x_1 \in T_0$, and evidentely, $x_jx_{j'} - x_ix_{i'} \in T_{b/2}$.

Finally, assume $\vec{\mathfrak{F}}_{b/2-m}$ is isomorphic to $\vec{\mathfrak{S}}_3^1$. Thus we have to consider the subdigraph containing the arcs $(2, 1)$ and $(1, 3)$. Inspection gives us $x_jx_{j'} - x_ix_{i'} = x_1(x_3 - x_2)$. However both, x_1 and $x_3 - x_2$ lie in T_0. So we find again $x_jx_{j'} - x_ix_{i'} \in T_0$. This completes the discussion of possible cases, and concludes the proof. ☐

Finally, we record a similar result for even prime powers. However, this time we must not distinguish between several classes of even prime powers.

Lemma 13. *Let $\vec{\mathfrak{H}}$ be a simple digraph with non-negative cyclomatic number. There exists a constant $q_{13} = q_{13}(\vec{\mathfrak{H}})$ such that every even prime power $q \geq q_{13}$ with $q \equiv 1 \bmod e(\vec{\mathfrak{H}})$ lies in $\mathcal{I}_{\vec{\mathfrak{H}}}$.*

Proof. The argument of Lemma 9 can easily be transfered to the case of even prime powers. In particular, we have to use Lemma 5 instead of Lemma 4 to ensure the existence of an appropriate k-tuple $\underline{x}$. Furthermore, the essential observation that -1 lies in the subgroup T is trivial for even q: in fields of even order we always have $-1 = 1$. ☐

Summing up the results from this section, we obtain the following observation.

Corollary 14. *For every simple digraph $\vec{\mathfrak{H}}$ with non-negative cyclomatic number the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ is non-empty and different from $\{1\}$.*

Proof. Let $q_{14} = q_{14}(\vec{\mathfrak{H}})$ be the supremum of the constants q_9, q_{12} and q_{13}. By virtue of Dirichlet's theorem there exists a prime p larger than q_{14} such that $q \equiv 1 \bmod e(\vec{\mathfrak{H}})$ holds. However, exactly one of the existence lemmas stated in this section applies to q. Thus $\mathcal{I}_{\vec{\mathfrak{H}}}$ contains q and satisfies the claim. $\square$

4 PBD–closure

The above discussion ensures the existence of prime powers in the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ of admissible values. In order to study the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ in greater detail we require the concept of pairwise balanced designs.

Consider a positive integer n and a subset K of the positive integers. A *pairwise balanced design* $PBD(n, K)$ is a pair $(V, \mathcal{F})$ consisting of an n-set V and a collection $\mathcal{F}$ of subsets $F \subseteq V$ (called *blocks*) such that every pair of distinct elements lies in exactly one block of $\mathcal{F}$ and all block sizes belong to K.

The *PBD-closure* of a given set K of positive integers consists of all integers n admitting a pairwise balanced design $PBD(n, K)$. Consequently, the set K is said to be *PBD-closed* iff K equals its PBD-closure. For a rigorous treatment of pairwise balanced designs and related topics, the reader should consult e.g. [3].

Examining the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ for a given digraph $\vec{\mathfrak{H}}$, we obtain the following result.

Lemma 15. *For every simple digraph $\vec{\mathfrak{H}}$, the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ is PBD-closed.*

Proof. According to Lemma 1, we may assume that $\vec{\mathfrak{H}}$ has non-negative cyclomatic number. Let n be an integer from the PBD-closure of $\mathcal{I}_{\vec{\mathfrak{H}}}$. Thus we find a pairwise balanced design $(V, \mathcal{F})$ of order n and block sizes from $\mathcal{I}_{\vec{\mathfrak{H}}}$. For every block $F = \{x_1, \ldots, x_{|F|}\} \in \mathcal{F}$, let $\mathcal{G}^F = \{\vec{\mathfrak{G}}^F_{x_1}, \ldots, \vec{\mathfrak{G}}^F_{x_{|F|}}\}$ be an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_{|F|}$ by an $\vec{\mathfrak{H}}$-family $\vec{\mathfrak{G}}^F$ of size $(|F| - 1)/e(\vec{\mathfrak{H}})$.

For brevity, the set of all blocks $F \in \mathcal{F}$ containing a fixed element x is said to be the *flower* on x in $\mathcal{F}$ and denoted by $\mathcal{F}(x)$. Let $\vec{\mathfrak{G}}_x$ be the union of all the digraphs $\vec{\mathfrak{G}}^F_x$ with $F \in \mathcal{F}(x)$. Obviously, $\vec{\mathfrak{G}}_x$ is again idempotent and an $\vec{\mathfrak{H}}$-family of size $(n-1)/e(\vec{\mathfrak{H}})$. Thus, $\vec{\mathfrak{G}}_x$ has just $e(\vec{\mathfrak{G}}_x) = n - 1$ arcs.

Due to the definition of pairwise balanced designs, every pair x,y of distinct elements from V belongs to exactly one block $F \in \mathcal{F}$. In $\mathcal{G}^F$ there exists precisely one digraph

$\vec{\mathfrak{G}}_z^F$ containing the arc (x, y). Hence, $\vec{\mathfrak{G}}_z$ is the only page in $\mathcal{G}$ containing (x, y) and, consequently, $\mathcal{G}$ is a decomposition of $\vec{\mathfrak{D}}_n$.

Furthermore, let $\vec{\mathfrak{G}}_x$ and $\vec{\mathfrak{G}}_y$ be two distinct digraphs in $\mathcal{G}$. There is exactly one block F in $\mathcal{F}$ containing both, x and y. Since $\mathcal{G}^F$ is an orthogonal decomposition, the union of $\vec{\mathfrak{G}}_x^F$ and $\vec{\mathfrak{G}}_y^F$ contains a digon. Due to our construction, this digon lies in the union of $\vec{\mathfrak{G}}_x$ and $\vec{\mathfrak{G}}_y$, too. This shows that the union of any two distinct pages in $\mathcal{G}$ contains at least (and thus exactly) one digon. $\square$

A set K of positive integers is said to be *eventually periodic* with period π iff, with some integer $r \in K$ all sufficiently large integers $n \equiv r \bmod \pi$ lie in K, too. The notion of eventual periodic sets was introduced by Wilson [17] who proved the following criterion which is among the most interesting general theorems in design theory.

Theorem 16 (Wilson). *Let K be a non-empty PBD-closed set different from $\{1\}$. Then K is eventually periodic with period $\beta(K) = g.c.d\{n(n-1) : n \in K\}$. In addition, K has period $\pi = \beta(K)/2$ iff π is odd and $\pi \equiv 0 \bmod \alpha(K)$ holds, where $\alpha(K) = g.c.d.\{n-1 : n \in K\}$.*

On applying Wilson's theorem to the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ we are able to verify the following property.

Lemma 17. *For every simple digraph $\vec{\mathfrak{H}}$ with non-negative cyclomatic number, the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ is eventually periodic with period $e(\vec{\mathfrak{H}})$.*

Proof. The eventual periodicity of $\mathcal{I}_{\vec{\mathfrak{H}}}$ follows immediately from Lemma 15 and Wilson's theorem. It remains to determine a period of $\mathcal{I}_{\vec{\mathfrak{H}}}$. By Lemma 1, we have $n - 1 \equiv 0 \bmod e(\vec{\mathfrak{H}})$ for every $n \in \mathcal{I}_{\vec{\mathfrak{H}}}$. Hence, $\beta(\mathcal{I}_{\vec{\mathfrak{H}}})$ is divisible by $e(\vec{\mathfrak{H}})$. Suppose, $e(\vec{\mathfrak{H}})$ is even. By Lemma 8 we find two primes $p, q \geq q_{14}$ with $p \equiv q \equiv 1 \bmod e(\vec{\mathfrak{H}})/2$ and $g.c.d.\{p(p-1), q(q-1)\} = e(\vec{\mathfrak{H}})$. Both, p and q are odd and relatively prime to $e(\vec{\mathfrak{H}})/2$. Therefore, $e(\vec{\mathfrak{H}})$ divides $p-1$ as well as $q-1$. It turns out that $p, q \in \mathcal{I}_{\vec{\mathfrak{H}}}$ and $\beta(\mathcal{I}_{\vec{\mathfrak{H}}}) = e(\vec{\mathfrak{H}})$ holds.

We now come to the case in which $e(\vec{\mathfrak{H}})$ is odd. This time, $\beta(\mathcal{I}_{\vec{\mathfrak{H}}})$ is divisible by $2e(\vec{\mathfrak{H}})$. Again by Lemma 7, there are primes $p, q \in \mathcal{I}_{\vec{\mathfrak{H}}}$ with $g.c.d.\{p(p-1), q(q-1)\} = 2e(\vec{\mathfrak{H}})$ such that $\beta(\mathcal{I}_{\vec{\mathfrak{H}}}) = 2e(\vec{\mathfrak{H}})$. Moreover, $\alpha(\mathcal{I}_{\vec{\mathfrak{H}}})$ is divisible by $e(\vec{\mathfrak{H}})$, too. Hence $\alpha(\mathcal{I}_{\vec{\mathfrak{H}}})$ is either $e(\vec{\mathfrak{H}})$ or $2e(\vec{\mathfrak{H}})$ depending on the existence of even integers in $\mathcal{I}_{\vec{\mathfrak{H}}}$.

In order to find even integers in $\mathcal{I}_{\vec{\mathfrak{H}}}$, consider the Euler totient function $\phi(n)$ providing the number of positive integers $m \leq n$ with $g.c.d.\{m, n\} = 1$. Since $e(\vec{\mathfrak{H}})$ is odd, we obtain

$$2^{\phi(e(\vec{\mathfrak{H}}))} \equiv 1 \bmod e(\vec{\mathfrak{H}})$$

due to the Euler-Fermat Theorem (see e.g. [11]). By Lemma 13 there is a positive integer λ with $2^{\lambda\phi(e(\vec{\mathfrak{H}}))} \in \mathcal{I}_{\vec{\mathfrak{H}}}$. Thus we obtain $\alpha(\mathcal{I}_{\vec{\mathfrak{H}}}) = e(\vec{\mathfrak{H}})$. Finally, Wilson's theorem settles our claim. □

We are now in the position to establish our main result that the set $\mathcal{I}_{\vec{\mathfrak{H}}}$ contains almost all integers n satisfying the necessary conditions given by Lemma 1. We record this as follows:

Theorem 18. *Let $\vec{\mathfrak{H}}$ be a simple digraph with non-negative cyclomatic number. There exists a constant $n_{18} = n_{18}(\vec{\mathfrak{H}})$ such that for every $n \geq n_{18}$ with $n \equiv 1 \mod e(\vec{\mathfrak{H}})$ there is an idempotent orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by an $\vec{\mathfrak{H}}$-family.*

5 Conclusions

Let $\vec{\mathfrak{H}}$ be a simple digraph with $v(\vec{\mathfrak{H}})$ vertices and $e(\vec{\mathfrak{H}})$ arcs. In the preceding sections we proved the existence of an orthogonal decomposition by an $\vec{\mathfrak{H}}$-family for all sufficiently large complete digraphs whenever $e(\vec{\mathfrak{H}}) \geq v(\vec{\mathfrak{H}})$ holds. On the other hand, it is easy to check similar to Lemma 2 that there is no orthogonal decomposition by $\vec{\mathfrak{H}}$-families if $e(\vec{\mathfrak{H}}) \leq v(\vec{\mathfrak{H}}) - 2$. The remaining case, namely $e(\vec{\mathfrak{H}}) = v(\vec{\mathfrak{H}}) - 1$ is of special interest. Here an orthogonal decomposition by an $\vec{\mathfrak{H}}$-family will only exist if this family is the digraph $\vec{\mathfrak{H}}$ itself. As pointed out in Section 1, this problem is unsolved in general, and the methods used in this article do not apply to this class of digraphs. Fortunately, the portion of simple digraphs with cyclomatic number -1 is considerably small.

Theorem 19. *For almost every simple digraph $\vec{\mathfrak{H}}$ there exists a constant $m_{19} = m_{19}(\vec{\mathfrak{H}})$ such that for every $m \geq m_{19}$ there is an orthogonal decomposition by $m\vec{\mathfrak{H}}$.*

Proof. Suppose $\vec{\mathfrak{H}}$ has non-negative cyclomatic number. Choose m_{19} such that $m_{19}e(\vec{\mathfrak{H}}) + 1 \geq n_{18}$ holds. By Theorem 18 there exists an orthogonal decomposition of $\vec{\mathfrak{D}}_n$ by $m\vec{\mathfrak{H}}$ if $n = me(\vec{\mathfrak{H}}) + 1 \geq n_{18}$, i.e. $m \geq m_{19}$ holds.

It remains to show that almost all simple digraphs have non-negative cyclomatic number. Let $u(n, b)$ and $l(n, b)$ denote the numbers of unlabeled and labeled simple digraphs with n vertices and b arcs, respectively. Moreover, let $u(n)$ and $l(n)$ be the total numbers of unlabeled and labeled simple digraphs with n vertices. It is easily verified, that

$$l(n, b) = \binom{\binom{n}{2}}{b} 2^b$$

and

$$l(n) = \sum_{b=0}^{\infty} l(n,b) = 3^{\binom{n}{2}}$$

hold. In addition, it is well-known that almost every simple digraph has trivial automorphism group, i.e. the proportion $n!u(n)/l(n)$ tends to 1 for $n \to \infty$ (cf. [4]).

Finally, let $u^-(n)$ and $l^-(n)$ denote the numbers of unlabeled and labeled simple digraphs with n vertices and negative cyclomatic number, respectively. We have

$$l^-(n) = \sum_{b=0}^{n-1} l(n,b) = \sum_{b=0}^{n-1} \binom{\binom{n}{2}}{b} 2^b \leq \sum_{b=0}^{n-1} \binom{n}{2}^b 2^b \leq n^{2n} = 3^{2n \log_3 n}.$$

This implies

$$0 \leq \frac{u^-(n)}{u(n)} \leq \frac{l^-(n)}{u(n)} = \frac{n!l^-(n)}{l(n)} \frac{l(n)}{n!u(n)} \leq 3^{3n \log_3 n - \binom{n}{2}} \frac{l(n)}{n!u(n)} = o(1) \frac{l(n)}{n!u(n)}$$

and consequently $u^-(n)/u(n)$ tends to 0 for $n \to \infty$. This concludes the proof. $\square$

The statement of Theorem 19 is remarkable since it is widely believed that there exists an orthogonal decomposition of a complete digraph by almost all simple digraphs. Hence, the constant $m_{19}(\vec{\mathfrak{H}})$ is expected to be one for almost all $\vec{\mathfrak{H}}$.However, a positive answer to this conjecture requires a proof which does not use Wilson's theorem on eventually periodic sets.

References

[1] B. Alspach, K. Heinrich, and G. Liu. Orthogonal factorizations of graphs. In J.H. Dinitz and D.R. Stinson, editors, *Contemporary Design Theory*, chapter 2, pages 13–40. J. Wiley, New York, 1992.

[2] F.E. Bennett and L. Wu. On minimum matrix representation of closure operations. *Discr. Appl. Math.*, 26:25–40, 1990.

[3] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory.* BI, Mannheim, 1985.

[4] P.J. Cameron. Automorphism groups of graphs. In L.W. Beineke and R.J. Wilson, editors, *Selected topics in graph theory*, volume 2, pages 89–127. Academic Press, London, 1983.

[5] J. Demetrovics, Z. Füredi, and G.O.H. Katona. Minimum matrix representations of closure operations. *Discr. Appl. Math.*, 11:115–128, 1985.

[6] J. Demetrovics and G.O.H. Katona. Extremal combinatorial problems in relational database. In *Fundamentals of computation theory*, volume 117 of *Lecture Notes in Computer Science*, pages 110–119. Springer, Berlin, 1981.

[7] B. Ganter and H.-D.O.F. Gronau. On two conjectures of Demetrovics, Füredi and Katona on partitions. *Discrete Math.*, 88:149–155, 1991.

[8] A. Granville, H.-D.O.F. Gronau, and R.C. Mullin. On a problem of hering concerning orthogonal double covers of K_n. *J. Comb. Theory*, A(72):345–350, 1995.

[9] F. Hering. Balanced pairs. *Ann. Discrete Math.*, 20:177–182, 1984.

[10] F. Hering and M. Rosenfeld. Problem number 38. In K. Heinrich, editor, *Unsolved Problems: Summer Research Workshop in Algebraic Combinatorics.* Simon Fraser University, 1979.

[11] A.N. Parshin and I.R. Shafarevich. *Number Theory.* Springer, Berlin, 1990.

[12] A. Rausche. On the existence of special block designs. *Rostock. Math. Kolloq.*, 35:13–20, 1988.

[13] R.Lidl and H.Niederreiter. *Finite fields.* Cambridge University Press, Cambridge, 1987.

[14] W.M. Schmidt. *Equations over finite fields.* Springer, Berlin, 1976.

[15] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. USA*, 34:204–207, 1948.

[16] R.M. Wilson. Cyclotomy and difference families in elementary abelian groups. *J. Number Theory*, 4:17–42, 1972.

[17] R.M. Wilson. An existence theory for pairwise balanced designs II. *J. Comb. Theory (A)*, 13:246–270, 1972.

[18] R.M. Wilson. Construction and uses of pairwise balanced designs. In M. Hall Jr. and J.H. van Lint, editors, *Combinatorics*, volume 55 of *Math. Centre Tracts*, pages 18–41. Mathematisch Centrum, Amsterdam, 1974.

[19] R.M. Wilson. An existence theory for pairwise balanced designs III. *J. Comb. Theory (A)*, 18:71–79, 1975.