https://doi.org/10.18453/rosdok_id00005832

[gs-odc1h, July 12, 2006]

Orthogonal Covers by Multiplication Graphs

By

Hans-Dietrich O.F. Gronau and Markus Schmidmeier

Abstract. Let K be the complete oriented graph on the finite set of vertices A. A family $\mathcal{G} = \{G_a : a \in A\}$ of spanning subgraphs of K is an *orthogonal cover* provided every arrow of K occurs in exactly one G_a and for every two elements $a, b \in A$, the graphs G_a and G_b^{op} have exactly one arrow in common. Gronau, Grüttmüller, Hartmann, Leck and Leck (2002) have observed that if A has the structure of a finite ring and if $f \in A$ is such that both $f + 1$ and $f - 1$ are units, then the family, obtained by taking for G_0 the multiplication graph of f and for G_a the rotation of G_0 by a, defines an orthogonal cover on K. In this manuscript we assume that A is a finite abelian group and proceed to

(i) generalize this construction to arbitrary endomorphisms of the underlying group and describe the possible graphs,
(ii) introduce a duality on the set of orthogonal covers and
(iii) give detailed descriptions of the covers in the case where A is cyclic or elementary abelian.

1. Introduction.

Let $K = K(A)$ be the complete oriented graph with vertex set A. A family $\mathcal{G} = (G_a)_{a \in A}$ of spanning subgraphs (called *pages*) of K is an *orthogonal cover* if the following two conditions hold.

(1) Every arrow in K belongs to exactly one of the pages (cover property) and
(2) for any pair (a, b) in A, the pages G_a and G_b^{op} have exactly one arrow in common (orthogonality).

The purpose of this manuscript is to investigate a large class of orthogonal covers. For this we assume that the index set A is equipped with the structure of a finite abelian group. Then we can assign to each arrow $\alpha : s \to t$ its *length* $\ell(\alpha) = t - s$, and we can measure the distance between two arrows. In particular, the *offset* $\varphi(\alpha) = t' - s$

2000 Mathematics Subject Classific.: 5B15 (primary), 5B40, 5E20 (secondary)
Keywords: orthogonal cover, ODC, graph decomposition, Fitting's Lemma

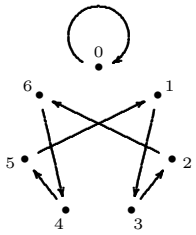
measures the distance between the arrow α and the corresponding arrow $\alpha' : s' \to t'$ of negative length. It turns out that for an orthogonal cover $\mathcal{G}$, the length and offset functions are bijections, and by exchanging length and offset we arrive at the *dual* cover, $D\mathcal{G}$, which we study in Section 2.

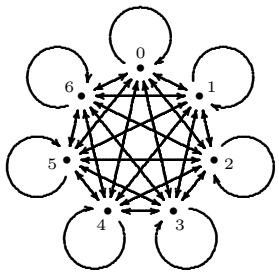
If G is a spanning subgraph of K and $a \in A$, then another spanning subgraph

$$G_a \ = \ \{(s + a \to t + a) : (s \to t) \in G\}$$

is obtained from G by rotation by a. (Here, as usual in this manuscript, a subgraph is given by the set of its arrows.) We say that the family $\mathcal{G} = \{G_a \ : \ a \in A\}$ is *group generated* by G, and that G is the *starter* for the family $\mathcal{G}$. We write $\mathcal{G} = \langle G \rangle$. In Section 3 we decide for which maps $f : A \to A$ the graph G of f is the starter for an orthogonal cover. Here is an example:

Example 1.1. Let A be the ring of integers modulo 7, K the complete oriented graph on A and G the spanning subgraph of K given by the graph of the map $\mu_3 : A \to A, a \mapsto 3a$. Then the rotations of G form an orthogonal cover for K.

G : 

K : 

The possible shapes of a graph which gives rise to an orthogonal cover is the topic of Section 4. Such a graph will be the product of a tree and a disjoint union U of cycles.

While the shape of the tree is easy to determine, the determination of the cycle type of U requires more attention. In Sections 5 and 6 we deal with the cases where A is elementary abelian and cyclic, respectively.

As application of our results, consider the corresponding covering problem for complete *unoriented* graphs. If C is such a graph with underlying set of vertices A, then a collection $\mathcal{G} = (G_i)_{i \in A}$ of spanning subgraphs of C is an *orthogonal double cover (ODC)* provided (i) every edge of C belongs to exactly two of the pages (double cover property) and (ii) any two distinct pages intersect in exactly one edge (orthogonality). For the history of ODCs, motivation and an overview of the state of the art we refer the reader to [2].

The construction of ODCs with pages of a given shape is of particular interest, and our results on orthogonal covers lend themselves to this purpose: From an orthogonal cover $\mathcal{G} = (G_a)_a$ an ODC is obtained by removing from each page G_a the loop (which is unique as we will see below) and by replacing each of the remaining arrows by an edge.

2. Two Self Dualities

If $\mathcal{G} = (G_a)$ is an orthogonal cover, then so is the family $\mathcal{G}^{\mathrm{op}} = (G_a^{\mathrm{op}})$ consisting of the opposite graphs. Clearly $(\mathcal{G}^{\mathrm{op}})^{\mathrm{op}} = \mathcal{G}$ holds, so taking opposite graphs is a self duality on the set of orthogonal covers.

In this section we introduce a second self duality D for group generated orthogonal covers, it is given by exchanging length and offset functions. Recall from [2, 2.1] the following equivalent characterisation of an orthogonal cover in terms of length and offset.

Lemma 2.1. *Let A be a finite abelian group and K the complete oriented graph on A. A spanning subgraph $G \subset K$ is a starter for an orthogonal cover if and only if G satisfies the following two conditions.*

- (1′) *For every $a \in A$ there is exactly one arrow $\alpha \in G$ of length $\ell(\alpha) = a$ (length condition) and*
- (2′) *for every $b \in A$ there is exactly one arrow $\beta \in G$ of offset $\varphi(\beta) = b$ (offset condition).* ✓

Note that because of (1′), the offset of the arrow α in (2′) is defined. In fact, length and offset define two bijections

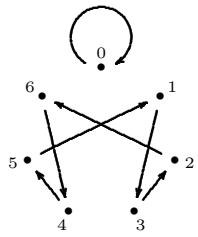
$$\ell, \varphi : \quad G \longrightarrow A$$

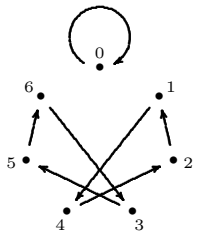
between the arrows in G and the elements of A. By reversing their role, that is to say by taking for each arrow $\alpha : s \to s + \ell(\alpha)$ in G a corresponding arrow $D\alpha : s \to s + \varphi(\alpha)$ in DG, we define the *dual* of the orthogonal cover $\mathcal{G}$:

$$D\mathcal{G} = \langle DG \rangle, \quad \text{where} \quad DG = \{D\alpha : \alpha \in G\}$$

Thus, we replace any two arrows $(s \to t)$ and $(s' \to t')$ in G where the length of the second is the negative of the length of the first by two corresponding arrows $(s \to t')$ and $(s' \to t)$ in DG. The length of the arrow $(s \to t') \in DG$ is the offset for the arrow $(s \to t) \in G$, and conversely.

Example 2.2. Here is the dual of the starter of the orthogonal cover in Example 1.1. Note that the cycle types of G and DG are different.

G : 

DG : 

With G also DG is the starter for an orthogonal cover. The following result is a consequence of Lemma 2.1:

PROPOSITION 2.3. *Let $\mathcal{G}$ be an orthogonal cover of K with starter G.*

1. *The dual graph DG is the starter for an orthogonal cover $D\mathcal{G}$ of K.*
2. *The orthogonal covers $\mathcal{G}$ and $DD\mathcal{G}$ coincide.* ✓

An orthogonal cover $\mathcal{G}$ is *self dual* if $\mathcal{G}$ and $D\mathcal{G}$ coincide.

LEMMA 2.4. 1. *If $\mathcal{G}$ is a self dual orthogonal cover then each page coincides with its dual page.*

2. *If A is an elementary abelian 2-group, that is if $a + a = 0$ holds for all $a \in A$, then any group generated orthogonal cover is self dual.*

Proof. 1. Each page has a unique arrow α of length 0, the loop. This arrow satisfies $\alpha = D\alpha$, and hence in a self dual covering, the page containing α can only correspond to itself under duality.
2. If A is an elementary abelian 2-group, then each arrow is equal to its dual. ✓

Combining the two dualities $\mathcal{G} \mapsto \mathcal{G}^{\rm op}$ and D, then any given orthogonal cover $\mathcal{G}$ gives rise to a sequence of orthogonal covers

$$\cdots\ (D\mathcal{G}^{\rm op})^{\rm op},\ D\mathcal{G}^{\rm op},\ \mathcal{G}^{\rm op},\ \mathcal{G},\ D\mathcal{G},\ (D\mathcal{G})^{\rm op},\ D((D\mathcal{G})^{\rm op}),\ \cdots$$

3. Orthogonal Covers Based on Maps

Let A be an abelian group and $f : A \to A$ a (set) map. Then $\langle f\rangle = (\mathrm{graph}(f)_a)_{a\in A}$ is a family of spanning subgraphs of $K(A)$.
We ask: For which maps $f : A \to A$ is the family $\langle f\rangle$ an orthogonal cover for $K(A)$?

Definition. We call a graph G *polycyclic* if G is a union of cycles with pairwise disjoint vertex sets. The partition listing the cycle lengths is the *cycle type* of G.

Example 3.1. The graph of any bijection is polycyclic. In particular, the multiplication maps $\mu_3, \mu_4 : \mathbb{Z}/(p^7) \to \mathbb{Z}/(p^7)$ in Example 2.2 are polycyclic and have cycle types $(6, 1)$ and $(3, 3, 1)$, respectively.

PROPOSITION 3.2. *Let A be a finite abelian group, $f : A \to A$ an even map, and K the complete oriented graph on A.*

1. *$\mathcal{G} = \langle f \rangle$ is an orthogonal cover for K if and only if the following two conditions are satisfied.*
   (1″) The map $f - 1_A$ is a bijection.
   (2″) The map $f + 1_A$ is a bijection.
2. *The orthogonal cover $\mathcal{G}$ is polycyclic if and only if the map f is in addition bijective.*

Clearly, a map $f : A \to A$ is *even* provided $f(-a) = -f(a)$ holds for all $a \in A$. In particular, every group homomorphism is even.

Proof. We only show the first assertion. Note that the length condition $(1')$ requires that the length function $\ell : A \to A, a \mapsto f(a) - a$, is a bijection. Thus, conditions $(1')$ and $(1'')$ are equivalent for a graph based starter. Assume now that in addition $f : A \to A$ is an even map. If $\alpha : s \to t$ is an arrow in the graph of f, then the (unique) arrow of negative length is $(-s \to -t)$ and hence the offset for α is $(-t) - s = -(f + 1_A)(s)$. Thus, the offset condition $(2')$ is equivalent to $(2'')$. ✓

COROLLARY 3.3. *Let A be an elementary abelian 2-group, that is, $a + a = 0$ holds for all $a \in A$. The graph of a map f defines an orthogonal cover if and only if the map $f - 1_A$ is bijective.*

Proof. Since A is an elementary abelian 2-group, any map $A \to A$ is even. If $f - 1_A$ is bijective, then so is $f + 1_A$ and the claim follows from Proposition 3.2 ✓

We return to our study of the dualities D and $\mathcal{G} \mapsto \mathcal{G}^{\mathrm{op}}$.

PROPOSITION 3.4. *Let A be a finite abelian group and $\mathcal{G}$ an orthogonal cover given by a map $f : A \to A$.*

1. *The dual cover $D\mathcal{G}$ is given by the negative map $-f : a \mapsto -f(a)$.*
2. *If $\mathcal{G}$ is polycyclic then f is bijective and the opposite cover is given by the inverse map $f^{-1} : a \mapsto f^{-1}(a)$.*

Proof. 1. An arrow $(a \to f(a)) = (a \to a + (f - 1_A)(a)) \in \mathrm{graph}(f)$ gives rise to the corresponding arrow $(a \to a + (-(f + 1_A)(a))) = (a \to -f(a))$ in the dual $D(\mathrm{graph}(f))$ of the graph of f: hence $D\mathcal{G} = \langle -f \rangle$.

2. If $\mathcal{G}$ is polycyclic, then the map f is bijective by Proposition 3.2, and the opposite of an arrow $a \mapsto b = f(a)$ is the arrow $b \mapsto a = f^{-1}(b)$. ✓

COROLLARY 3.5. *An orthogonal cover given by a map f is self dual if and only if for every $a \in A$ the condition $f(a) = -f(a)$ holds. In particular, the orthogonal cover given by the zero map is self dual. Also, if A is an elementary abelian 2-group then any orthogonal cover given by the graph of any map is self dual.*

Proof. If f is a map defining an orthogonal cover $\mathcal{G}$, then so is $-f$. The condition $f = -f$ makes sure that $\mathcal{G}$ is self dual. Conversely, let $\mathcal{G} = \langle f \rangle$ be an orthogonal cover which is self dual. Then the page $G = \operatorname{graph}(f)$ coincides with its dual page DG by Lemma 2.4, and this page is just $DG = \operatorname{graph}(-f)$ by Proposition 3.4. ✓

4. The shape of the starters

We recall Fitting's Lemma (see [1, Proposition 11.7]): Let $f : A \to A$ be an endomorphism of a module A of finite length. There is a direct sum decomposition $A = A' \oplus A''$ of this module such that

1. both submodules A' and A'' are invariant under f, so f restricts to endomorphisms f' and f'' of A' and A'', respectively,
2. the endomorphism f' acts nilpotently on A' so there is $n \in \mathbb{N}$ such that $f'^n = 0$, and
3. the map f'' acts as a bijection on A''.

In fact, A' and A'' can be taken to be the kernel and the image of f^n, respectively. The result applies in particular to finite abelian groups, so any group map $f : A \to A$ decomposes A into a product $A = A' \times A''$ such that assertions 1.–3. hold.

Using Fitting's Lemma as a guideline, we first recall the shape of graphs of nilpotent maps, then comment on graphs of bijections and finally consider products of both graphs.

LEMMA 4.1. *Suppose that f is a nilpotent endomorphism on a finite module A.*

1. *The graph of f forms the starter of an orthogonal cover.*
2. *The shape of the graph is a tree with a loop at the root 0.*
3. *The elements in A not in the image of f correspond to leaves of the tree.*
4. *The elements in the image of f are the branch points; each branch point has $|\operatorname{Ker} f| = |\{a \in A : f(a) = 0\}|$ incoming arrows.*
5. *The points at a given height $s \geq 1$ over the root correspond to the elements in $\operatorname{Ker} f^s \setminus \operatorname{Ker} f^{s-1}$.*

Proof. 1. Note that the maps $f + 1_A$ and $f - 1_A$ are invertible with inverse $1_A - f + f^2 - \cdots \pm f^{n-1}$ and $1_A + f + f^2 + \cdots + f^{n-1}$, respectively, where n is such that $f^n = 0$. The claim follows from Proposition 3.2.
2. Since f is nilpotent, the graph of f is a tree.
3. and 4. The equation $f(x) = a$ has a solution if and only if $a \in \operatorname{Im} f$; if the equation has at least one solution, then the number of solutions is equal to the number of solutions of the homogeneous equation $f(x) = 0$, which is $|\operatorname{Ker} f|$.
5. The elements in $\operatorname{Ker} f^s$ correspond to the points in the tree of height at most s. ✓

In the case where f acts as a bijection on A, i.e., if $A = A''$ holds, then the graph G of f is polycyclic and Proposition 3.2 describes when G is the starter of an orthogonal cover. We discuss examples of polycyclic starters in Sections 5 and 6.

In the mixed case, the graph of f is the product of the two graphs of the restrictions $f' = f|_{A'}$ and $f'' = f|_{A''}$. We pause to study products of spanning subgraphs in general.
Let $\mathcal{G}' = \{G'_i : i \in A'\}$ and $\mathcal{G}'' = \{G''_j : j \in A''\}$ be families of spanning subgraphs for the complete oriented graphs K' and K'', respectively. Define the product of two arrows $\alpha : s \to t$ and $\beta : u \to v$ to be the arrow between the products, $(\alpha, \beta) : (s, u) \to (t, v)$; the product $G' \times G''$ of two graphs G' and G'' to be the set of all products of arrows; and the product of two families $\mathcal{G}'$ and $\mathcal{G}''$ of spanning subgraphs the family of all graph products. We omit the proof of the following result which is straightforward:

LEMMA 4.2. 1. *The product $\mathcal{G} = \mathcal{G}' \times \mathcal{G}''$ of two families of spanning subgraphs on the complete graphs K' and K'' forms an orthogonal cover on the complete graph $K = K' \times K''$ if and only if both families $\mathcal{G}'$ and $\mathcal{G}''$ form orthogonal covers on K' and K'', respectively.*
2. *If G' and G'' are starters for orthogonal covers $\mathcal{G}'$ and $\mathcal{G}''$ then $G' \times G''$ is a starter for the product $\mathcal{G}' \times \mathcal{G}''$.*
3. *In the situation of 1., the orthogonal cover $\mathcal{G}$ is polycyclic if and only if both covers $\mathcal{G}'$ and $\mathcal{G}''$ are polycyclic.* ✓

Whenever two pages $G'_i \in \mathcal{G}'$ and $G''_j \in \mathcal{G}''$ contain cycles, the cycle decomposition of the product is under control.

PROPOSITION 4.3. *Given cycles $C' \subset G'_i$ and $C'' \subset G''_j$ of length c' and c'',respectively, then the corresponding subset $C' \times C'' \subset G'_i \times G''_j$ is the disjoint union of* $\gcd(c', c'')$ *cycles of length* $\operatorname{lcm}(c', c'')$.

Proof. The group $\mathbb{Z}$ of integers acts on the underlying sets of C' and C'' by rotation along the arrows; via this operation these sets become the $\mathbb{Z}$-modules $\mathbb{Z}/(c')$ and $\mathbb{Z}/(c'')$. The direct sum $\mathbb{Z}/(c') \oplus \mathbb{Z}/(c'')$ is as a $\mathbb{Z}$-module isomorphic to $\mathbb{Z}/(\gcd(c', c'')) \oplus \mathbb{Z}/(\mathrm{lcm}(c', c''))$. Since $\gcd(c', c'')$ is a divisor of $\mathrm{lcm}(c', c'')$, the $\mathbb{Z}$-action decomposes this set into $\gcd(c', c'')$ many orbits of length $\mathrm{lcm}(c', c'')$. ✓

Products of group generated orthogonal covers are well behaved with respect to the duality.

LEMMA 4.4. *If $\mathcal{G}'$ and $\mathcal{G}''$ are group generated orthogonal covers, then also the products $\mathcal{G}' \times \mathcal{G}''$ and $D\mathcal{G}' \times D\mathcal{G}''$ are group generated and*

$$D(\mathcal{G}' \times \mathcal{G}'') \;=\; D\mathcal{G}' \times D\mathcal{G}''.$$

Proof. Suppose $\mathcal{G}' = \langle G' \rangle$ and $\mathcal{G}'' = \langle G'' \rangle$ are group generated orthogonal covers on the abelian groups A' and A'', respectively. Then $\mathcal{G}' \times \mathcal{G}'' = \langle G' \times G'' \rangle$ and $D\mathcal{G}' \times D\mathcal{G}'' = \langle DG' \times DG'' \rangle$ both are group generated covers on the abelian group $A' \times A''$.

A typical arrow in a page $G'_i \times G''_j$ in $\mathcal{G}' \times \mathcal{G}''$ has the form $(s', s'') \to (t', t'')$ where $s' \to t'$ and $s'' \to t''$ are arrows in G'_i and G''_j, respectively. Let $u' \to v'$ and $u'' \to v''$ be the corresponding arrows of negative length, so $s' \to v'$, $u' \to t'$ are arrows in DG'_i, and $s'' \to v''$, $u'' \to t''$ are arrows in DG''_j. Then $(u', u'') \to (v', v'')$ is the arrow in $G'_i \times G''_j$ which has the negative of the length of $(s', s'') \to (t', t'')$, so the two corresponding arrows in $D(G'_i \times G''_j)$ are $(s', s'') \to (v', v'')$ and $(u', u'') \to (t', t'')$. Clearly, they correspond to the pairs $(s' \to v', s'' \to v'')$, $(u' \to t', u'' \to t'')$ in $DG'_i \times DG''_j$. ✓

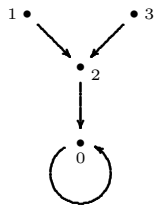
Returning to the situation where $\mathcal{G} = \langle f \rangle$ is group generated by the graph of an endomorphism $f : A \to A$, our findings yield the following description of the shape of the starter:

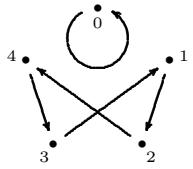
PROPOSITION 4.5. *Let $A = A' \oplus A''$ be a decomposition of A such that the endomorphism $f : A \to A$ restricts to a nilpotent map $f' : A' \to A'$ on A' and a bijection $f'' : A'' \to A''$ on A'', as in the introduction of this section.*

1. *The graph of f is the starter for an orthogonal cover if and only if both maps $f'' + 1_{A''}$ and $f'' - 1_{A''}$ are bijections on A''.*
2. *Moreover,* $\mathrm{graph}(f)$ *is the product of the tree* $\mathrm{graph}(f')$ *and the disjoint union of cycles,* $\mathrm{graph}(f'')$.
3. *The shape of* $\mathrm{graph}(f)$ *is obtained by replacing every point in the union of cycles* $\mathrm{graph}(f'')$ *by a copy of the tree* $\mathrm{graph}(f')$ *with the*

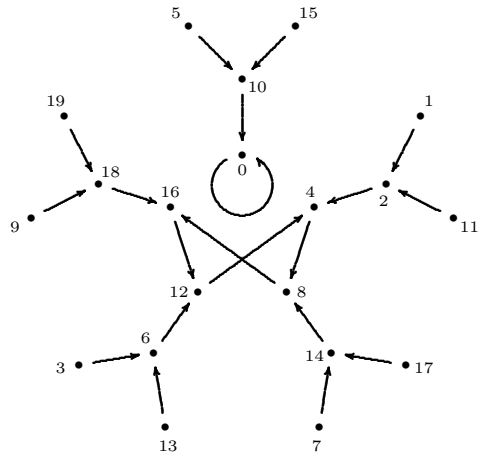
loop at the root deleted, and with the roots linked by the cycles in graph(f''). ✓

Example 4.6. Consider the orthogonal covers for $\mathbb{Z}/(4)$ and $\mathbb{Z}/(5)$ generated by the graphs of multiplication by 2. Here are the starters:

G_4 : 

G_5 : 

The product $G_4 \times G_5$ is the starter for an orthogonal cover on $\mathbb{Z}/(20)$, it is the graph of the map given by multiplication by 2:

$G_4 \times G_5$: 

5. Elementary Abelian Groups

Let A be the elementary abelian p-group of order p^n, so A is the direct sum of n copies of the field $\mathbb{F}_p$ of p elements. In this section we survey several constructions for polycyclic orthogonal covers with cycle type under control. We illustrate these constructions in the example where $A = \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5$.

5.1. **Fields.** The field $\mathbb{F}_{p^n}$ of p^n elements has underlying abelian group A and its unit group is cyclic of order $p^n - 1$. If x is a unit of order $d|(p^n-1)$ then the graph of the multiplication map $\mu_x : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, a \mapsto xa$, consists of the zero orbit and p^{n-1}/d orbits of length d. We conclude using Proposition 3.2:

Lemma 5.1. *Let $x \neq \pm 1$ be a unit in the finite field $\mathbb{F}_{p^n}$ and let d be the multiplicative order of x. Then $\mathcal{G} = \langle \mu_x \rangle$ is an orthogonal cover for*

the complete graph on p^n vertices. This cover is polycyclic of cycle type $(d^{p-1/d}, 1)$, so there are $\frac{p-1}{d}$ cycles of length d, and the loop. ✓

Example 5.2. If $p^n = 5^3$ then the only possible cycle lengths in multiplication graphs for $\mathbb{F}_{p^n}$ are the divisors of $5^3 - 1 = 124$. In particular, no divisor is a multiple of 3 or a multiple of $p = 5$, or a multiple of any odd prime different from 31. Thus under this construction no cycle length which is a multiple of any odd prime $\neq 31$ can possibly occur.

5.2. **Polynomial rings.** For q a power of p, consider the polynomial ring $A = \mathbb{F}_q[T]/(T^s)$. Recall that in this ring, p-th powers are computed using the Frobenius homomorphism: $(a + bT + cT^2 + \cdots)^p = (a^p + b^pT^p + c^pT^{2p} + \cdots)$ and by simplifying the result modulo T^s. Units in A are the elements with nonzero constant term. It is easy to see that if $s \leq p$ then the order of any unit is a divisor of $(q-1)p$, and each divisor can be realized: If $t|(q-1)$ and if $a \in \mathbb{F}_q$ has order t, then a and $a + T$ have order t and tp, respectively. We have the following more general result:

LEMMA 5.3. *Let $x = x_0 + x_1T + \cdots + x_{s-1}T^{s-1}$ be a unit in the polynomial ring $R = \mathbb{F}_q[T]/(T^s)$ where q is a power of p.*

1. *The order d of x is a divisor of $D = (q-1)p^{\lceil \log_p s \rceil}$ where $\lceil v \rceil$ denotes the smallest integer $\geq v$.*
2. *Any divisor of D can be realized by a polynomial of type $x = (a + bT^c)$ where $b \in \{0, 1\}$ and $c \geq 1$.*
3. *The collection $\langle \mu_x \rangle$ is an orthogonal cover for the complete graph on q^s vertices if and only if $x_0 \neq \pm 1$.*

Proof. For any polynomial $x \in R$, the $p^{\lceil \log_p s \rceil}$th power of x is a constant polynomial, say y, and the given exponent is minimal so that this property holds for all x. Since $y \neq 0$ in the field of q elements, we have $y^{q-1} = 1$. Note that any possible order can be realized by a polynomial of type $a + bT^c$ where a in $\mathbb{F}_q$, $b \in \{0, 1\}$, and $c \geq 1$. In fact if u is a nonnegative integer, $(1 + T^c)^{p^u} = 1 + T^{cp^u} = 1$ holds if and only if $cp^u \geq s$ or $u \geq \log_p \frac{s}{c}$.
For the third assertion we need to show for a unit x that $x + 1$ and $x - 1$ are invertible. This is equivalent to require that $x_0 \neq \pm 1$. ✓

Example 5.4. Also the polynomial ring $R = \mathbb{F}_5[T]/(T^3)$ has underlying abelian group $A = \mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5$. According to the lemma, every unit in R has order a divisor of $(q-1)p = 4 \cdot 5 = 20$; however, units of order $1, 5, 2, 10$ have constant term ± 1 and do not give rise to an orthogonal cover. The polynomial $x = 2 + T$ has order 20 and its multiplication graph is the starter for an orthogonal cover on A of

cycle type $(20^6, 4, 1)$. Note that also the polynomial $y = 2 + T^2$ has order 20 and its multiplication graph is the starter for an orthogonal cover on A. But the second graph has cycle type $(20^5, 4^6, 1)$. (The two graphs differ because T^2 acts trivially on the polynomials in TR.)
Thus we see that the order of a unit does not determine the cycle type uniquely.

5.3. **Products.** Also products studied in the previous section can be used to realize certain cycle types.

Example 5.5. An element (a, b) of order 12 in the product $\mathbb{F}_{5^2} \times \mathbb{F}_5$ is obtained by taking for a an element of order 3 in $\mathbb{F}_{5^2}$ and for b an element of order 4 in $\mathbb{F}_5$, say $b = 2$. Since the graph of μ_a has cycle type $(3^8, 1)$ and the graph of μ_b has type $(4, 1)$, the graph of $\mu_{(a,b)}$ is a starter for an orthogonal cover of cycle type $(12^8, 4, 3^8, 1)$, by Proposition 4.3.

5.4. **Matrix rings.** Which orders are possible for a bijection f acting on an elementary abelian p-group? Under the extra assumption that f is a group endomorphism we have the following criterion.

Lemma 5.6. *Let f be an endomorphism of the elementary abelian group of order p^n, so f is given by an $n \times n$-matrix with coefficients in $\mathbb{F}_p$.*

1. *The map f is the starter of an orthogonal cover if and only if neither $+1$ nor -1 is an eigenvalue of f.*
2. *f is the starter of a polycyclic orthogonal cover if and only if neither 0 nor $+1$ nor -1 is an eigenvalue of f.*
3. *If f is invertible then the order of f is a divisor of $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.*

Proof. According to Proposition 3.2, the graph of f is the starter of a (polycyclic) orthogonal cover if the maps $f - 1_A$, $f + 1_A$ (and f itself) are bijections. In case f is given by a matrix M, the corresponding condition is that M has no eigenvalue equal to $+1$, -1 (and 0).
It is well known (and easy to see by counting systems of linearly independent columns) that the matrix group $\mathrm{Gl}_n(\mathbb{F}_p)$ has order $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$. By Lagrange's Theorem, the order of any unit is a divisor of this number. ✓

Example 5.7. Here is another orthogonal cover on the complete graph on $\mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5$ where some cycles have length a multiple of 3. The permutation matrix $M = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$ has order 3 but it also has eigenvalue 1 and hence is not the starter for an orthogonal cover. However, the product DM with the diagonal matrix $D = \left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ is a matrix of

multiplicative order 12 with no eigenvalue equal to $+1$, -1 or 0. The orthogonal cover spanned by DM has cycle type $(12^{10}, 4, 1)$; the orbit of length 4 consists of the vectors $\binom{1}{4}{2}$, $\binom{3}{2}{1}$, $\binom{4}{1}{3}$ and $\binom{2}{3}{4}$.

Example 5.8. Let p be a prime number greater than 5 and different from 31. Since $p \nmid (5^3-1)(5^3-5)(5^3-5^2)$, no multiple of p can possibly occur in the cycle type of any orthogonal cover given by an endomorphism of $\mathbb{F}_5 \oplus \mathbb{F}_5 \oplus \mathbb{F}_5$

6. The integers modulo m

In this section we assume that $A = \mathbb{Z}/(m)$ is the ring of integers modulo m and describe the possible orthogonal covers generated by multiplication graphs of elements. We assume that m has prime factor decomposition $m = p_1^{t_1} \cdots p_s^{t_s}$ where the p_i are pairwise different prime numbers and all t_j are positive numbers. According to the Chinese Remainder Theorem [3, 12B Theorem 2 and E4], there is an isomorphism of rings:

$$\mathbb{Z}/(m) \;\cong\; \mathbb{Z}/(p_1^{t_1}) \times \cdots \times \mathbb{Z}/(p_s^{t_s}).$$

Let $x \in A$ correspond under this isomorphism to the tuple $(x_1, \ldots, x_s)$ where $x_i \in \mathbb{Z}/(p_i^{t_i})$. We may rearrange the factors of A in such a way that there is $1 \le r \le s$ such that the elements $x_i \in \mathbb{Z}/(p_i^{t_i})$ are units for $1 \le i \le r$ and nilpotent elements or zero if $i > r$. Thus, A is the product $A = A' \times A''$ where

$$A' = \mathbb{Z}/(p_1^{t_1}) \times \cdots \times \mathbb{Z}/(p_r^{t_r}) \quad \text{and} \quad A'' = \mathbb{Z}/(p_{r+1}^{t_{r+1}}) \times \cdots \times \mathbb{Z}/(p_s^{t_s}).$$

If $x = (x', x'')$ with $x' \in A'$ and $x'' \in A''$ then x'' is nilpotent or zero and x' a unit. The multiplication graph given by x'' is a tree and its shape is determined by Lemma 4.1, while the graph of $\mu_{x'}$ is a disjoint union of cycles for which we will describe the cycle type below. Then the multiplication graph for the pair $x = (x', x'')$ is the product as described in Proposition 4.5.

The element x' itself is given by the tuple $(x_1, \ldots, x_r)$ where each entry is a unit. Hence the cycle type for $\mu_{x'}$ is given by the cycle types for the μ_{x_i} by Proposition 4.3. Thus it remains to describe the cycle type of μ_x where x is a unit in the ring of integers $\mathbb{Z}/(p^t)$ where p is a prime. (We may assume without loss of generality that $p \neq 2$ because no unit in the ring $\mathbb{Z}/(2^t)$ generates an orthogonal cover by Proposition 3.2.)

We recall from [3, Section 24B] the following facts about the group of units in $\mathbb{Z}/(p^t)$.

LEMMA 6.1. *Let $A = \mathbb{Z}/(p^t)$ where $p \neq 2$ is a prime number and denote by U the group of units in A.*

1. *The element $1 + p$ generates a subgroup of U of order p^{t-1}.*
2. *U is a cyclic group of order $\varphi(p^t) = (p-1)p^{t-1}$.* ✓

We can now describe the graph of μ_x if x is a unit in A.

PROPOSITION 6.2. *Let $p \neq 2$ be a prime number, $A = \mathbb{Z}/(p^t)$, U the group of units in A, and $x \in U$.*

1. *A is the disjoint union $A = U \,\dot\cup\, pU \,\dot\cup\, \cdots \,\dot\cup\, p^{t-1}U \,\dot\cup\, \{0\}$.*
2. *If x generates U then the graph of μ_x has cycle type*
$$\big(((p-1)p^{t-1}),\ ((p-1)p^{t-2}),\ \cdots,\ (p-1), 1\big),$$
corresponding to the decomposition of A in 1.
3. *In general if $x = g^v$ for a generator $g \in U$, then the graph of μ_x has cycle type*
$$\big(\gcd(v,\varphi(p^t))^{\varphi(p^t)/\gcd(v,\varphi(p^t))}, \gcd(v,\varphi(p^{t-1}))^{\varphi(p^{t-1})/\gcd(v,\varphi(p^{t-1}))}, \ldots, 1\big),$$
more precisely, U decomposes into $\varphi(p^t)/\gcd(v,\varphi(p^t))$ many orbits of length $\gcd(v,\varphi(p^t))$, pU into $\varphi(p^{t-1})/\gcd(v,\varphi(p^{t-1}))$ many orbits of length $\gcd(v,\varphi(p^{t-1}))$, etc.

Remark. Compare this result with Example 5.4: The order of a unit in $\mathbb{Z}/(p^n)$ determines the cycle decomposition for $\mathbb{Z}/(p^n)$ uniquely, but the order of a unit in $\mathbb{F}_p[T]/T^s$ does not.

Proof. 1. The filtration $0 \subset p^{t-1}A \subset \cdots \subset pA \subset A$ gives rise to the decomposition of $A = U \,\dot\cup\, pU \,\dot\cup\, \cdots \,\dot\cup\, \{0\}$ as a disjoint union since $p^sU = p^sA \backslash p^{s+1}A$.
2. Multiplication by p^s maps the orbit $(1, x, x^2, \ldots)$ which consists of all $p^{t-1}(p-1)$ elements in U onto the orbit $(p^s, p^sx, p^sx^2, \ldots)$ which consists of all $p^{t-s-1}(p-1)$ elements in p^sU. In particular, each set p^sU consists of a single orbit under multiplication by x.
3. If $x = g^v$ for a generator g of U, then the orbit of x has length $\gcd(v, \varphi(p^t))$ (which is the multiplicative order of x), so in the multiplication graph for x, the set U decomposes into $\varphi(p^t)/\gcd(v, \varphi(p^t))$ many orbits.
The canonical map $\mathbb{Z}/(p^t) \to \mathbb{Z}/(p^{t-s})$ maps g to a generator $\bar g$ of $U(\mathbb{Z}/(p^{t-s}))$ and hence x to the power $\bar x = \bar g^v$. Thus, $\bar x$ has order $\gcd(v, \varphi(p^{t-s}))$ and hence multiplication by $\bar x$ decomposes $U(\mathbb{Z}/(p^{t-s}))$ into $\varphi(p^{t-s})/\gcd(v, \varphi(p^{t-s}))$ many orbits.
The module map $\mathbb{Z}/(p^{t-s}) \to \mathbb{Z}/(p^t), a \mapsto p^sa$, bijectively maps every orbit in $U(\mathbb{Z}/(p^{t-s}))$ into a corresponding orbit in $p^sU(\mathbb{Z}/(p^t))$,

hence multiplication by x (or $\bar{x}$) decomposes $p^sU(\mathbb{Z}/(p^t))$ into $\varphi(p^{t-s})/\gcd(v,\varphi(p^{t-s}))$ many orbits, each of length $\gcd(v,\varphi(p^{t-s}))$. ✓

Example 6.3. Consider the ring A of integers modulo 637. Prime factor decomposition yields $637 = 7^2 \cdot 13$, so $A \cong \mathbb{Z}/(7^2) \times \mathbb{Z}/(13)$. The group of units U_{7^2} of the first factor is cyclic of order 42, a generator is 3. Thus, multiplication by 3 decomposes $\mathbb{Z}/(7^2)$ into three orbits of length $6\cdot 7$, 6 and 1. The group of units U_{13} of the second factor is cyclic of order 12, generated by 2; multiplication by 2 decomposes $\mathbb{Z}/(13)$ into two orbits of length 12 and 1. We obtain from the Chinese Remainder Theorem that $x = 444$ corresponds to $(3,2)$ under the canonical isomorphism $\mathbb{Z}/(637) \cong \mathbb{Z}/(7^2) \times \mathbb{Z}/(13)$. The lengths of the orbits in the product and their multiplicities are obtained from Lemma 4.3 as follows:

Component Product	Number of Points	1st Factor Orbits	1st Factor Len	2nd Factor Orbits	2nd Factor Len	Product Orbits	Product Len
$U_{7^2} \times U_{13}$	504	1	42	1	12	6	84
$7U_{7^2} \times U_{13}$	72	1	6	1	12	6	12
$\{0\} \times U_{13}$	12	1	1	1	12	1	12
$U_{7^2} \times \{0\}$	42	1	42	1	1	1	42
$7U_{7^2} \times \{0\}$	6	1	6	1	1	1	6
$\{0\} \times \{0\}$	1	1	1	1	1	1	1
	637					16	

Thus the orthogonal cover $\langle \mu_{444} \rangle$ has cycle type $(84^6, 42, 12^7, 6, 1)$.

Example 6.4. Again for the ring $A = \mathbb{Z}/(637) \cong \mathbb{Z}/(7^2) \times \mathbb{Z}/(13)$, let's take in each factor a unit of order 3, for example, $30 \in \mathbb{Z}/(7^2)$ and $3 \in \mathbb{Z}/(13)$. The Chinese Remainder Theorem yields an element $x = 471$ of order 3 in A. Now the graph of μ_x has cycle decomposition $(3^{212}, 1)$:

Component Product	Number of Points	1st Factor Orbits	1st Factor Len	2nd Factor Orbits	2nd Factor Len	Product Orbits	Product Len
$U_{7^2} \times U_{13}$	504	14	3	4	3	$14 \cdot 4 \cdot 3$	3
$7U_{7^2} \times U_{13}$	72	2	3	4	3	$2 \cdot 4 \cdot 3$	3
$\{0\} \times U_{13}$	12	1	1	4	3	4	3
$U_{7^2} \times \{0\}$	42	14	3	1	1	14	3
$7U_{7^2} \times \{0\}$	6	2	3	1	1	2	3
$\{0\} \times \{0\}$	1	1	1	1	1	1	1
	637					213	

References

[1] F. W. Anderson and K. R. Fuller, *Rings and categories of modules,* Springer GTM **13**, 2nd edition, 1992.

[2] H.-D. O. F. Gronau, M. Grüttmüller, S. Hartmann, U. Leck, and V. Leck, *On orthogonal double covers of graphs,* Designs, codes and cryptography **27**, 49–91, (2002).

[3] L. N. Childs, *A concrete introduction to higher algebra,* 2nd edition, Springer UTM (1995).

Address of the Authors:

Institut für Mathematik
Universität Rostock
Universitätsplatz 1
18055 Rostock
Germany

e-mail:
gronau@uni-rostock.de

Mathematical Sciences
Florida Atlantic University
777 Glades Road
Boca Raton, Florida 33431
United States of America

e-mail:
markus@math.fau.edu