

## AUTOMORPHISMS OF DECOMPOSITIONS

TIM HANNAN\* — JOHN HARDING\*\*

*To Anatolij Dvurečenskij*

*(Communicated by Sylvia Pulmannová)*

ABSTRACT. In [HARDING, J.: *Decompositions in quantum logic*, Trans. Amer. Math. Soc. **348** (1996), 1839–1862] the author showed that the direct product decompositions of many different types of structures, such as sets, groups, vector spaces, topological spaces, and relational structures, naturally form orthomodular posets. When applied to the direct product decompositions of a Hilbert space, this construction yields the familiar orthomodular lattice of closed subspaces of the Hilbert space.

In this note we consider orthomodular posets FACT  $X$  of decompositions of a finite set  $X$ . We consider the structure of these orthomodular posets, such as their size, shape, connectedness, states, and begin a study of their automorphism groups in the context of the natural map  $\Gamma$  from the group of permutations of  $X$  to the automorphism group of FACT  $X$ .

We show  $\Gamma$  is an embedding except when  $|X|$  is prime or 4, and completely describe the situation when  $|X|$  has two or fewer prime factors, when  $|X| = 2^3$  and when  $|X| = 3^3$ . The bulk of our effort lies in a series of combinatorial arguments to show  $\Gamma$  is an isomorphism when  $|X| = 27$ . We conjecture that this is the case whenever  $|X|$  has sufficiently many prime factors of sufficient size, and hope that our arguments here might be adapted to the general case.

©2016  
 Mathematical Institute  
 Slovak Academy of Sciences

### 1. Introduction

A binary decomposition of a structure  $A$  consists of structures  $B, C$  and an isomorphism  $f: A \rightarrow B \times C$ . Another binary decomposition  $f': A \rightarrow B' \times C'$  is equivalent to the given one if there are isomorphisms  $u: B \rightarrow B'$  and  $v: C \rightarrow C'$  with  $f' = (u \times v) \circ f$  as shown below.

$$\begin{array}{ccc}
 & & B \times C \\
 & \nearrow f & \downarrow u \\
 A & & \\
 & \searrow f' & \downarrow v \\
 & & B' \times C'
 \end{array}$$

This equivalence of decompositions is different (finer) than that encountered in the Krüll-Schmidt theorem, where only the isomorphism classes of the factors are important. In the above definition of equivalence, the order of the factors and the way the isomorphism  $f$  decomposes the structure matter. This is analogous to the situation for onto homomorphisms  $f: A \rightarrow B$ , where equivalence could mean isomorphism of the images, or the existence of an isomorphism between

2010 Mathematics Subject Classification: Primary 81P10, 06C15, 08A35, 05E99, 51D20.

Keywords: orthomodular poset, automorphism, direct product decomposition, Wigner's Theorem.

the images compatible with the homomorphisms. While the second approach is more frequent when dealing with onto homomorphisms, it is the first usually encountered when dealing with decompositions. Our focus is the more refined equivalence for decompositions.

A small example may help. A 4-element set  $X = \{a, b, c, d\}$  has 8 equivalence classes of decompositions. One has as its representatives decompositions of  $X$  as a product of a 4-element set and a 1-element set. There are a proper class of such decompositions, but all are equivalent. Another has as its representatives decompositions of  $X$  as a product of a 1-element set and a 4-element set. There are 6 equivalence classes whose representatives decompose  $A$  as a product of two 2-element sets. To see these can be different, consider one bijection  $f$  from  $X$  to a product of two 2-element sets where  $f(a)$  and  $f(b)$  have the same first component, and another bijection  $g$  from  $X$  to a product of two 2-element sets where  $g(a)$  and  $g(b)$  have different first components. The decompositions given by  $f$  and  $g$  will be inequivalent.

**DEFINITION 1.1.** For a structure  $A$ , let  $\text{FACT } A$  be the set of all equivalence classes of binary decompositions of  $A$ .

When dealing with a set  $X$ , each equivalence class of decompositions has a unique representative  $f: X \rightarrow X/\theta_1 \times X/\theta_2$  where  $\theta_1$  and  $\theta_2$  are equivalence relations on  $X$  and the natural map  $f$  given by these relations is a bijection. Such pairs of equivalence relations are called factor pairs [5].

**THEOREM 1.2.** For a set  $X$ ,  $\text{FACT } X = \{(\theta_1, \theta_2) : (\theta_1, \theta_2) \text{ is a factor pair}\}$ .

We next consider the matter of defining structure on the set  $\text{FACT } A$ . We require the following well-known notion from the study of quantum logic [22, 28].

**DEFINITION 1.3.** An orthomodular poset (abbreviated: OMP) is a bounded poset  $P$  with bounds  $0, 1$  and a unary operation  $'$  that is order inverting and period two, such that the following conditions hold with regard to the existence and behavior of certain joins and meets. Here,  $x \perp y$  means  $x \leq y'$  and is read “ $x$  is orthogonal to  $y$ .”

- (1) For each  $x \in P$ ,  $x \wedge x'$  exists and is  $0$ , and  $x \vee x'$  exists and is  $1$ .
- (2) If  $x \perp y$ , then the join  $x \vee y$  exists.
- (3) If  $x \perp y'$ , then  $x \vee (x \vee y)' = y'$ .

We next put structure on  $\text{FACT } A$ . For a binary decomposition  $f: A \rightarrow B \times C$ , there is a related decomposition  $f': A \rightarrow C \times B$ , and this naturally defines a unary operation  $'$  on  $\text{FACT } A$ . For a ternary decomposition  $h: A \rightarrow B \times C \times D$ , there are binary decompositions  $h_1: A \rightarrow B \times (C \times D)$  and  $h_2: A \rightarrow (B \times C) \times D$  given in an obvious way. We define a relation  $\leq$  on  $\text{FACT } A$  by setting one equivalence class of binary decompositions to be  $\leq$  another if there is a ternary decomposition  $h: A \rightarrow B \times C \times D$  with the first equivalence class containing  $h_1: A \rightarrow B \times (C \times D)$  and the second  $h_2: A \rightarrow (B \times C) \times D$ . The following was established in [12].

**THEOREM 1.4.** For  $A$  a set, group, ring, vector space, topological space, or relational structure,  $\text{FACT } A$  is an OMP.

The structure on  $\text{FACT } X$  for a set  $X$  can be described using factor pairs [12]. We choose to use the orthogonality relation  $\perp$  as primitive rather than  $\leq$  as it appears frequently in the sequel. Of course, these are inter-definable using the orthocomplementation  $'$ . We also make use of the fact that an OMP is isomorphic to its order dual to express the partial ordering and orthogonality in what seems a more natural way. We note that equivalence relations  $\theta, \psi$  permute, or commute, if  $\theta \circ \psi = \psi \circ \theta$ .

**THEOREM 1.5.** When  $\text{FACT } X$  is realized as factor pairs, we have  $(\theta_1, \theta_2)' = (\theta_2, \theta_1)$  and  $(\theta_1, \theta_2) \perp (\psi_1, \psi_2)$  iff  $\theta_1 \subseteq \psi_2$ ,  $\psi_1 \subseteq \theta_2$ , and  $\theta_1$  permutes with  $\psi_1$ .

FACT  $A$  has been studied in a number of papers. In [12], the construction and its basic properties were introduced; it was shown that several familiar methods for constructing OMPs were instances of this construction; two related constructions of OMPs from relation algebras and symmetric lattices were given and used to show every modular ortholattice arises this way; and an example was given of a finite OMP that cannot be embedded into any FACT  $A$ . In [13] the blocks (maximal Boolean subalgebras) of FACT  $A$  were described via Boolean sheaves, and the regularity of FACT  $A$  established. In [14] direct physical motivation for the use of FACT  $A$  in theoretical quantum mechanics was given. In [15] an example of a FACT  $A$  with no states was given, and it was shown there is a finite OMP that can be embedded into FACT  $A$  for an infinite set  $A$  but not for any finite set  $A$ . In [16] FACT  $A$  was considered in a general categorical context. A survey of these results is given in [17]. In [18,19] FACT  $A$  is related to various categorical treatments of quantum mechanics and quantum logic [1,21].

The purpose of this paper is to study finer properties of the OMPs FACT  $X$  for the case that  $X$  is a finite set. We do this as a means of beginning a study of such properties for various kinds of structures due to connections to quantum logic, and as we believe the decompositions of a finite set form an object of basic interest, much as the partition lattice of a finite set. In particular, we study properties of automorphisms.

To frame the discussion, we state the following easily proved result that relates the automorphism group  $\text{AUT}(A)$  of the structure  $A$ , to the automorphism group  $\text{AUT}(\text{FACT } A)$  of the OMP FACT  $A$ . We note that an automorphism of an OMP is an order isomorphism that preserves the orthocomplementation.

**THEOREM 1.6.** *There is a group homomorphism  $\Gamma: \text{AUT}(A) \rightarrow \text{AUT}(\text{FACT } A)$  where  $\Gamma(\alpha)$  takes the equivalence class of the decomposition  $f: A \rightarrow B \times C$  to the equivalence class of the decomposition  $f \circ \alpha: A \rightarrow B \times C$ .*

There are several results known regarding automorphisms of structures FACT  $A$ . For a Hilbert space  $\mathcal{H}$ , the structure FACT  $\mathcal{H}$  is the orthomodular lattice of closed subspaces [12]. Ulhorn’s [30] version of Wigner’s theorem shows that the automorphisms of FACT  $\mathcal{H}$  are given by the unitary and anti-unitary operators on  $\mathcal{H}$ . In a series of papers by Chevalier and Ovchinnikov [7–9, 27] this was generalized to show the automorphisms of FACT  $V$  for a vector space  $V$  are given by isomorphisms and dual isomorphisms of the subspace lattice of  $V$ . In the finite-dimensional case, the fundamental theorem of projective geometry then provides a description of the automorphism group of FACT  $V$  in terms of the general linear group of  $V$ .

In this paper, the second section begins with some elementary combinatorial computations to find the number of atoms, number of blocks, size of blocks, and so forth, for the structures FACT  $X$  for a finite set  $X$  and FACT  $V$  for a finite-dimensional vector space  $V$ . For sets with  $p^k$  elements for some prime  $p$ , and for finite-dimensional vector spaces over finite fields, these are seen to give interesting classes of  $(n, m)$ -homogeneous OMPs [29], that is, ones where each block has  $m$  atoms and each atom is in  $n$  blocks. Several less basic combinatorial properties of these structures are also considered, such as the relationship between FACT  $V$  when  $V$  is considered as a vector space and FACT  $V$  when  $V$  is considered as a set. Many of the results of this section are used when we consider automorphisms.

In the third section, we consider basic properties of automorphisms of FACT  $X$  for a  $X$  a finite set. We show that if  $|X|$  is neither prime nor equal to 4, then the map  $\Gamma$  is an embedding. Calling the kernel of  $\Gamma$  the phase group of the structure, this says that except in some trivial cases, finite sets have trivial phase groups. We also show that the automorphism group of FACT  $X$  is transitive on the atoms in a strong way, moving any block to any other. We then completely describe the automorphism group of FACT  $X$  in the “small” cases where  $|X|$  has at most two prime factors, and where  $|X| = 8$ .

Automorphisms groups in these “small” cases are somewhat uninteresting as the structures involved are too poor to allow control over automorphisms. This is particularly true when  $|X|$  has just two prime factors as  $\text{FACT } X$  is the horizontal sum of 4-element Boolean algebras. In the smallest case where  $|X|$  has three prime factors, when  $|X| = 8$ ,  $\text{FACT } X$  is again a horizontal sum, but of more complex pieces. This kind of pathology with small size is familiar in quantum logic with most results about Hilbert spaces having exceptions in the case of dimension 2. We conjecture below that these pathologies vanish as the size of the set becomes sufficiently large.

**CONJECTURE 1.7.** *If  $X$  is a finite set with at least three prime factors greater than 2, then the map  $\Gamma: \text{AUT}(X) \rightarrow \text{AUT}(\text{FACT } X)$  is an isomorphism.*

In the fourth and fifth sections, we verify this conjecture in the case that  $|X| = 3^3$ . This is not an easy task. The structure  $\text{FACT } X$  has

$$5,001,134,190,558,105,600,000$$

atoms, and we are considering automorphisms of this structure. The proof proceeds in two steps. The first consists of showing each automorphism of  $\text{FACT } X$  induces an automorphism on the poset of regular equivalence relations on  $X$ , and is the content of Section 4. The second step shows that each automorphism of the poset of regular equivalence relations on  $X$  is given by a permutation of  $X$ , and is the content of Section 5. Both halves of the proof rely on a sequence of elementary combinatorial computations. The method of proof may extend to the more general setting, but will require further non-trivial effort.

In the sixth and final section, we make some remarks regarding group-valued states on the structures  $\text{FACT } X$  and  $\text{FACT } V$ , and discuss directions for possible further research.

## 2. Counting with sets and vector spaces

Here we employ some basic combinatorial techniques to describe properties such as the number of atoms in  $\text{FACT } X$  for a finite set  $X$ . We begin with a generalization of the notion of a factor pair described in the introduction. We call a sequence of equivalence relations  $(\theta_1, \dots, \theta_n)$  on a set  $X$  a factor  $n$ -tuple if the natural map  $X \rightsquigarrow X/\theta_1 \times \dots \times X/\theta_n$  is a bijection. Factor  $n$ -tuples can be described concretely for arbitrary sets [24], but the finite sets there is a very simple alternative description.

**LEMMA 2.1.** *Suppose  $(\theta_1, \dots, \theta_n)$  is an  $n$ -tuple of equivalence relations on a finite set  $X$  where  $\theta_i$  has  $m_i$  blocks. Then this is a factor  $n$ -tuple iff*

- (1)  $\theta_1 \cap \dots \cap \theta_n = \Delta$ .
- (2)  $|X| = m_1 m_2 \dots m_n$ .

**PROOF.** The first condition means the map  $X \rightsquigarrow X/\theta_1 \times \dots \times X/\theta_n$  is a one-one map, and  $\theta_i$  having  $m_i$  blocks means  $X/\theta_i$  has  $m_i$  elements.  $\square$

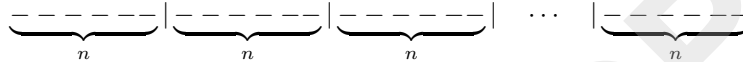
An equivalence relation that occurs as part of a factor pair, or equivalently as part of a factor  $n$ -tuple, is called a factor relation. We call one factor relation a companion of another if the pair forms a factor pair. Each factor relation on a set is regular, meaning that all its equivalence classes have the same cardinality, and each regular equivalence relation on a set is a factor relation. To see this, note that for a factor pair  $(\theta_1, \theta_2)$ , each equivalence class of  $\theta_1$  has  $|X/\theta_2|$  elements, and if  $\theta_1$  is regular, then enumerating the  $i^{\text{th}}$  equivalence class of  $\theta_1$  by  $(x_{ij})$  ( $j \in J$ ), we may define  $\theta_2$  to be all ordered pairs  $(x_{ij}, x_{kj})$  and so produce a factor pair  $(\theta_1, \theta_2)$ .

**PROPOSITION 2.2.** *Suppose a finite set  $X$  has  $mn$  elements. Then there are*

$$\frac{(mn)!}{m!(n!)^m}$$

*factor relations with  $m$  blocks of  $n$  elements each, and each has  $(n!)^{m-1}$  companions.*

**Proof.** There are  $(mn)!$  listings of the elements of  $X$ . The factor relations with  $m$  blocks of  $n$  elements each arise by taking the listings and inserting division lines after each batch of  $n$  elements, separating the listing of  $X$  into  $m$  groups of  $n$ . The order of the groups does not matter, and the order of the elements within the groupings does not matter, so we divide by  $m!$  and we divide by  $(n!)^m$ . This gives the formula for the number of factor relations with  $m$  blocks of  $n$  elements each.



Suppose  $\theta$  is a factor relation with  $m$  blocks of  $n$  elements each and  $\phi$  is a companion of  $\theta$ . Then  $\phi$  has  $n$  blocks of  $m$  elements each and each block of  $\phi$  has exactly one element of each block of  $\theta$ . We show  $\theta$  below with the blocks as rows.

$a_{11}$	$a_{12}$	$a_{13}$	$\cdots$	$a_{1n}$
$a_{21}$	$a_{22}$	$a_{23}$	$\cdots$	$a_{2n}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_{m1}$	$a_{m2}$	$a_{m3}$	$\cdots$	$a_{mn}$

One block of  $\phi$ , we call it the first, will contain  $a_{11}$ , one block, call it the second, will contain  $a_{12}$ , and so forth. To fill out the rest of the first block of  $\phi$  we must choose one element from each row of  $\theta$  after the first row, so there are  $n^{m-1}$  ways to choose the first block of  $\phi$ . Once the first block of  $\phi$  is chosen, we choose the second block by choosing one element from each of rows  $2, \dots, m$  of  $\theta$  not already chosen for the first block of  $\phi$ . So there are  $(n-1)^{m-1}$  ways to choose the second block, and so forth. In total, we have  $(n)^{m-1}(n-1)^{m-1}(n-2)^{m-1} \cdots (2)^{m-1}(1)^{m-1}$  ways to select  $\phi$ . But this simplifies to  $(n!)^{m-1}$  ways to choose  $\phi$ . □

**COROLLARY 2.3.** *If  $|X| = mn$  then the number of factor pairs  $(\theta_1, \theta_2)$  where  $\theta_1$  has  $m$  blocks of  $n$  elements each and  $\theta_2$  has  $n$  blocks of  $m$  elements each is given by*

$$\frac{(mn)!}{m!n!}$$

This lets us count the number of atoms in FACT  $X$  for any finite set. In general, the atoms will be of the form  $(\theta_1, \theta_2)$  where the blocks of  $\theta_1$  have a prime number of elements. Usually the atoms of FACT  $X$  will come in different flavors depending on the different primes that divide  $|X|$ . We can use the above to count the number of each flavor, but we keep it simple and limit ourselves to the following.

**COROLLARY 2.4.** *If  $|X| = p^k$  with  $p$  prime, then the number of atoms in FACT  $X$  is*

$$\frac{p^k!}{p!(p^{k-1})!}$$

We next turn to counting the blocks (maximal Boolean subalgebras) of FACT  $X$ . We again restrict attention to the case where  $|X| = p^k$  is a prime power, and call attention to the fact that we use the term block both for an equivalence class of an equivalence relation, and for a maximal Boolean subalgebra of an OMP. The key is the following result that follows from [13: Prop. 3.8] by noting that the directly indecomposable sets are those with a prime number of elements.

**COROLLARY 2.5.** *If  $X$  is a finite set, then the blocks of FACT  $X$  correspond to unordered versions of factor  $n$ -tuples  $(\theta_1, \dots, \theta_n)$  where each  $\theta_i$  has a prime number of blocks.*

Note, factor  $n$ -tuples correspond to blocks with a specific order to their atoms. Permuting a factor  $n$ -tuple gives a new factor  $n$ -tuple, but yields the same block.

**LEMMA 2.6.** *If  $|X| = p^k$  where  $p$  is prime, then the number of blocks in FACT  $X$  is*

$$\frac{p^k!}{k!(p!)^k}.$$

*Proof.* By Corollary 2.5 we want the number of factor  $k$ -tuples  $(\theta_1, \dots, \theta_k)$  where each  $\theta_i$  has  $p$  blocks with  $p^{k-1}$  elements each, divided by  $k!$ . For such a factor  $k$ -tuple,  $\theta_1 \cap \theta_2$  has  $p^2$  blocks of  $p^{k-2}$  elements each,  $\theta_1 \cap \theta_2 \cap \theta_3$  has  $p^3$  blocks of  $p^{k-3}$  elements each, and so forth. We build  $\theta_1, \theta_2, \dots, \theta_k$  with this in mind. By Proposition 2.2, the number of ways to choose  $\theta_1$  is given by

$$\frac{(p^k)!}{p!((p^{k-1})!)^{p-1}}.$$

With  $\theta_1$  chosen, we begin to construct  $\theta_2$ . To choose the first block of  $\theta_2$  we choose  $p^{k-2}$  elements from the  $p^{k-1}$  elements of the first block of  $\theta_1$ ,  $p^{k-2}$  elements from the  $p^{k-1}$  elements of the second block of  $\theta_1$ , and so forth. Using standard notation  $\binom{m}{n}$  for  $m$  choose  $n$ , we may choose the first block of  $\theta_2$  in the following number of ways.

$$\binom{p^{k-1}}{p^{k-2}}^p$$

Building the second block of  $\theta_2$  is similar, but from each of the  $p$  blocks of  $\theta_1$  we choose  $p^{k-2}$  of the  $p^{k-1} - p^{k-2} = (p-1)p^{k-2}$  elements in that block not already chosen. Building the third block of  $\theta_2$  is also similar, but from each of the  $p$  blocks of  $\theta_1$  we choose  $p^{k-2}$  of the  $p^{k-1} - 2p^{k-2} = (p-2)p^{k-2}$  elements not already chosen. As the order of the  $p$  blocks of  $\theta_2$  does not matter (dividing by  $p!$ ) we may choose  $\theta_2$  in the following number of ways.

$$\frac{1}{p!} \left[ \binom{pp^{k-2}}{p^{k-2}} \binom{(p-1)p^{k-2}}{p^{k-2}} \binom{(p-2)p^{k-2}}{p^{k-2}} \cdots \binom{p^{k-2}}{p^{k-2}} \right]^p$$

Setting  $u = p^{k-2}$  to aid legibility, this expression is equal to

$$\frac{1}{p!} \left[ \frac{p^{k-1}!}{((p-1)u)!u!} \frac{((p-1)u)!}{((p-2)u)!u!} \frac{((p-2)u)!}{((p-3)u)!u!} \cdots \frac{(3u)!}{(2u)!u!} \frac{(2u)!}{u!u!} \frac{u!}{0!u!} \right]^p$$

After simplification, given  $\theta_1$ , the number of ways to choose  $\theta_2$  equals

$$\frac{1}{p!} \left[ \frac{p^{k-1}!}{(p^{k-2}!)^p} \right]^p$$

Suppose  $\theta_1$  and  $\theta_2$  are chosen. Then  $\theta_1 \cap \theta_2$  has  $p^2$  blocks with  $p^{k-2}$  elements each. To construct the first block of  $\theta_3$  choose  $p^{k-3}$  elements from the  $p^{k-2}$  elements of each of these  $p^2$  blocks of  $\theta_1 \cap \theta_2$ . So there will be  $\binom{p^{k-2}}{p^{k-3}}^{p^2}$  ways to select the first block. Setting  $v = p^{k-3}$  and proceeding as above, the number of ways to construct  $\theta_3$  is given by

$$\frac{1}{p!} \left[ \frac{p^{k-2}!}{((p-1)v)!v!} \frac{((p-1)v)!}{((p-2)v)!v!} \frac{((p-2)v)!}{((p-3)v)!v!} \cdots \frac{(3v)!}{(2v)!v!} \frac{(2v)!}{v!v!} \frac{v!}{0!v!} \right]^{p^2}$$

So given  $\theta_1, \theta_2$ , the number of ways to choose  $\theta_3$  is

$$\frac{1}{p!} \left[ \frac{p^{k-2}!}{(p^{k-3}!)^p} \right]^{p^2}$$

Proceeding, the number of ways to choose  $\theta_1, \theta_2, \dots, \theta_k$  is

$$\frac{1}{p!} \left[ \frac{p^k!}{(p^{k-1}!)^p} \right]^1 \frac{1}{p!} \left[ \frac{p^{k-1}!}{(p^{k-2}!)^p} \right]^p \frac{1}{p!} \left[ \frac{p^{k-2}!}{(p^{k-3}!)^p} \right]^{p^2} \cdots \frac{1}{p!} \left[ \frac{p^2!}{(p!)^p} \right]^{p^{k-2}} \frac{1}{p!} \left[ \frac{p!}{(1!)^p} \right]^{p^{k-1}}$$

This simplifies to

$$\frac{1}{(p!)^k} \frac{p^k!}{(p^{k-1}!)^p} \frac{(p^{k-1}!)^p}{(p^{k-2}!)^{p^2}} \frac{(p^{k-2}!)^{p^2}}{(p^{k-3}!)^{p^3}} \cdots \frac{(p^3!)^{p^{k-3}}}{(p^2!)^{p^{k-2}}} \frac{(p^2!)^{p^{k-2}}}{(p!)^{p^{k-1}}} \frac{(p!)^{p^{k-1}}}{(1!)^{p^k}}$$

This is the number of ways to choose  $\theta_1, \dots, \theta_k$  where order matters. Dividing this by  $k!$  gives the number of blocks, and the result after noticing that many terms above cancel, is the following.

$$\frac{p^k!}{k!(p!)^k}.$$

This is the desired formula. □

**PROPOSITION 2.7.** *Suppose  $|X| = p^k$  with  $p$  prime. Then each block of FACT  $X$  has  $k$  atoms, and each atom belongs to the following number of blocks.*

$$\frac{p^{k-1}!}{(k-1)!(p!)^{k-1}}$$

*Proof.* As blocks of FACT  $X$  are given by factor  $k$ -tuples  $(\theta_1, \dots, \theta_k)$  where each  $\theta_i$  has  $p$  blocks, it follows from results from Corollary 2.5 that each block of FACT  $X$  has  $k$  atoms. Let  $A$  be the number of atoms and  $B$  the number of blocks in FACT  $X$ . Above we have seen

$$A = \frac{p^k!}{p!(p^{k-1}!)^p} \quad \text{and} \quad B = \frac{p^k!}{k!(p!)^k}.$$

As each block has  $k$  atoms in it, the average number of blocks an atom belongs to is

$$\frac{kB}{A} = \frac{p^{k-1}!}{(k-1)!(p!)^{k-1}}$$

Later, in Proposition 3.3, we will see that if  $|X|$  is a prime power, then there is an automorphism of FACT  $X$  taking any given atom to any other. It follows that all atoms are in the same number of blocks, so this average is realized by all atoms. □

**Remark 2.8.** An OMP is called  $(n, m)$ -homogeneous [29] if all of its blocks have  $m$  atoms and each atom is in  $n$  blocks. The above results show that if  $X$  is a set with  $p^k$  elements for some prime  $p$ , then FACT  $X$  is  $(n, m)$ -homogeneous where  $m = k$  and  $n$  is given in Proposition 2.7. In the next section we will see that this homogeneity arises in a very strong way, from the fact that given any two blocks with any sequencing of their atoms, there is an automorphism of FACT  $X$  taking the atoms of one block to the atoms of the other that respects the sequencing of these atoms. We call such an OMP strongly transitive. Any strongly transitive OMP is  $(n, m)$ -homogeneous, but not conversely, as is seen by taking the horizontal sum of two non-isomorphic  $(n, m)$ -homogeneous OMPs.

Factor pairs sharing a component, such as  $(\alpha, \gamma)$  and  $(\beta, \gamma)$ , play an important role in the study of automorphisms, and also in the structure of FACT  $A$ . The following result clarifies their situation.

**PROPOSITION 2.9.** *If  $\alpha, \beta$  are equivalence relations on a set  $X$ , with each having the same finite number  $k$  of blocks all with the same cardinality, then there is an equivalence relation  $\gamma$  so that both  $(\alpha, \gamma)$  and  $(\beta, \gamma)$  are factor pairs.*

**Proof.** We first consider the case where  $X$  is finite. Then  $\alpha$  partitions  $X$  into  $k$  pieces  $X_1, \dots, X_k$  with each piece having  $n$  elements, and  $\beta$  also partitions  $X$  into  $k$  pieces  $Y_1, \dots, Y_k$ , again with each piece having  $n$  elements. We will show there is a partition of  $X$  into  $n$  pieces  $Z_1, \dots, Z_n$  with each piece having  $k$  elements so that  $|X_i \cap Z_j| = |Y_i \cap Z_j| = 1$  for each  $i \leq k$  and  $j \leq n$ . This will establish the result in the case that  $X$  is finite.

**CLAIM 2.10.** *There is  $Z_1 = \{x_1, \dots, x_k\}$  with  $|X_i \cap Z_1| = |Y_i \cap Z_1| = 1$  for each  $i \leq k$ .*

**Proof.** Let  $S_p = \{i : X_p \cap Y_i \neq \emptyset\}$  for  $p = 1, \dots, k$ . Let  $\mathcal{S} = \{S_1, \dots, S_k\}$ . Take an arbitrary number  $m$  of these sets  $S_i$ , without loss of generality,  $S_1, \dots, S_m$ . We claim their union has at least  $m$  elements. As  $X$  is covered by the  $Y_i$ 's, it follows that the  $m$ -element set  $X_1 \cup \dots \cup X_m$  is covered by the  $Y_i$ 's and hence by the  $Y_i$ 's where  $i \in S_1 \cup \dots \cup S_m$ . As each  $Y_i$  has  $n$  elements, there must be at least  $m$  of the  $i$ 's belonging to  $S_1 \cup \dots \cup S_m$ . So  $\mathcal{S}$  satisfies the conditions for Phillip Hall's Marriage Theorem, so has a system of distinct representatives. This means we can choose distinct  $j_1, \dots, j_k$  so that  $j_i \in S_i$  for each  $i \leq k$ . This means  $X_i \cap Y_{j_i} \neq \emptyset$  for each  $i \leq k$ . So we can pick  $x_i \in X_i \cap Y_{j_i}$ . Set  $Z_1 = \{x_1, \dots, x_k\}$ .  $\square$

**CLAIM 2.11.** *There is a partition  $Z_1, \dots, Z_n$  of  $X$  with each  $Z_i$  having  $k$  elements, and such that  $|X_i \cap Z_j| = |Y_i \cap Z_j| = 1$  for each  $i \leq k$  and  $j \leq n$ .*

**Proof.** By induction on  $n$  for fixed  $k$ . Claim 1 shows we can find  $Z_1$  with  $k$  elements so that  $Z_1$  hits each  $X_i$  exactly once and each  $Y_i$  exactly once. Let  $X' = X - Z_1$ ,  $X'_i = X_i - Z_1$  and  $Y'_i = Y_i - Z_1$ . Then  $X'_1, \dots, X'_k$  and  $Y'_1, \dots, Y'_k$  are partitions of  $X'$  into  $(n - 1)$ -element pieces. By the inductive hypothesis we can find  $Z_2, \dots, Z_n$  partitioning  $X'$  into  $k$ -element pieces so that  $|X'_i \cap Z_j| = |Y'_i \cap Z_j| = 1$  for each  $i \leq k$  and  $2 \leq j \leq n$ . Then  $Z_1, \dots, Z_n$  has the desired properties.  $\square$

Having established the result for the finite case, the proof of the infinite case is identical using the infinite version of Phillip Hall's theorem (proved by the unrelated Marshall Hall). This result requires that we have finitely many infinite sets, which is the case as we have required  $\alpha, \beta$  to have finitely many blocks.  $\square$

We next turn our attention to FACT  $V$  for a vector space  $V$ . Noting that the decompositions of  $V$  are given by factor  $n$ -tuples  $(\theta_1, \dots, \theta_n)$  where each  $\theta_i$  is a vector space congruence, [13: Thm. 5.10] shows that if  $V$  is of finite dimension  $k$ , then the blocks of FACT  $V$  each have  $k$  atoms. If  $V$  is finite-dimensional and over a finite field, then  $V$  itself is finite, and we may employ counting techniques similar to those used for sets with FACT  $V$ . This will be our primary interest here. We begin with our basic representation for vector spaces, established in [12].

**THEOREM 2.12.** *For  $V$  a vector space, FACT  $V$  may be realized as the set of all ordered pairs of complementary subspaces  $(S, T)$  of  $V$ , meaning pairs with  $S \cap T = \{0\}$  and  $S + T = V$ , where  $(S, T)' = (T, S)$  and  $(S_1, T_1) \leq (S_2, T_2)$  iff  $S_1 \subseteq S_2$  and  $T_2 \subseteq T_1$ .*

FACT  $V$  for a vector space  $V$  may be viewed as a special case of other more general methods to construct OMPs, such as the OMP of idempotents of a ring, or as the OMP of certain complementary pairs of elements of a symmetric lattice [12].

**LEMMA 2.13.** *Let  $V$  be a  $k$ -dimensional vector space over an  $n$ -element field. Then*

- (1) Fact  $V$  has  $\frac{n^k - 1}{n - 1} n^{k-1}$  atoms.
- (2) Fact  $V$  has  $\frac{(n^k - 1)(n^k - n)(n^k - n^2) \dots (n^k - n^{k-1})}{k! (n - 1)^k}$  blocks.



(3) Each atom is in  $\frac{(n^k - n)(n^k - n^2)(n^k - n^3) \cdots (n^k - n^{k-1})}{(k-1)!n^{k-1}(n-1)^{k-1}}$  blocks.

Proof. There are  $n^k - 1$  non-zero elements in  $V$ . Each non-zero vector has  $n - 1$  non-zero scalar multiples, so each one-dimensional subspace has  $n - 1$  non-zero elements. Thus

$$\text{The number of 1-dim subspaces is: } \frac{n^k - 1}{n - 1} \tag{2.1}$$

By a general argument using annihilators, there are the same number of  $d$ -dimensional subspaces as  $(k - d)$ -dimensional subspaces, and this gives the following.

$$\text{The number of } (k-1)\text{-dim subspaces is: } \frac{n^k - 1}{n - 1} \tag{2.2}$$

Now each  $(k - 1)$ -dimensional subspace has  $n^{k-1} - 1$  non-zero vectors in it. So there are  $(n^k - 1) - (n^{k-1} - 1) = n^k - n^{k-1}$  non-zero vectors not in it. Each 1-dimensional subspace disjoint from a  $(k - 1)$ -dimensional subspace has  $n - 1$  non-zero vectors in it, so each  $(k - 1)$ -dimensional subspace has  $(n^k - n^{k-1}) / (n - 1) = n^{k-1}$  1-dimensional subspaces disjoint from it. Thus

$$\text{The number of atoms is: } \frac{n^k - 1}{n - 1} n^{k-1} \tag{2.3}$$

Applying Corollary 2.5 and [13: Thm. 5.10] to vector spaces, blocks of Fact  $V$  correspond to sets of  $k$  1-dimensional subspaces whose collective span is all of  $V$ . This means unordered bases, up to scalar multiples of the basis elements. There are  $(n^k - 1) / (n - 1)$  ways to choose the first basis element. Once chosen, we need a non-zero vector not in this space, so there are  $[(n^k - 1) - (n - 1)] / (n - 1) = (n^k - n) / (n - 1)$  ways to do this up to equivalence by scalar multiples. For the third, we need a non-zero vector not in the 2-dimensional span of what we have so far. There are  $[(n^k - 1) - (n^2 - 1)] / (n - 1) = (n^k - n^2) / (n - 1)$  ways to do this up to scalar multiples. In total there are the following number of ways to choose this ordered basis up to equivalence of scalar multiples.

$$\frac{n^k - 1}{n - 1} \frac{n^k - n}{n - 1} \frac{n^k - n^2}{n - 1} \frac{n^k - n^3}{n - 1} \cdots \frac{n^k - n^{k-1}}{n - 1} \tag{2.4}$$

So dividing out the order we then have

$$\text{The number of blocks is: } \frac{(n^k - 1)(n^k - n)(n^k - n^2) \cdots (n^k - n^{k-1})}{k!(n - 1)^k} \tag{2.5}$$

The average number of blocks each atom is in equals (the number of blocks) times (the number of atoms per block) divided by (the number of atoms), and there are  $k$  atoms in each block. So

$$\text{No. blocks each atom is in: } \frac{(n^k - n)(n^k - n^2)(n^k - n^3) \cdots (n^k - n^{k-1})}{(k - 1)!n^{k-1}(n - 1)^{k-1}} \tag{2.6}$$

Here we use a result from the following section that the automorphism group of FACT  $V$  is transitive on atoms. So the average number of blocks each atom is in is attained by each atom.  $\square$

We give several computations in specific cases.

**Example 2.14.** For  $V = \mathbb{Z}_2^3$ , FACT  $V$  has 28 atoms, 28 blocks, each block has 3 atoms, and each atom is in 3 blocks. For  $V = \mathbb{Z}_3^3$ , FACT  $V$  has 117 atoms, 234 blocks, each block has 3 atoms, and each atom is in 6 blocks. For  $X$  an 8-element set, FACT  $X$  has 840 atoms, 840 blocks, each block has 3 atoms and each atom is in 3 blocks. For  $X$  a 27-element set, things become very large. FACT  $X$  has  $27! / 3!9! = 5,001,134,190,558,105,600,000$  atoms,  $27! / 3!6^3$  blocks, each block has 3 atoms, and each atom is in 10,080 blocks.

These counting arguments provide key insight into FACT  $X$  for an 8-element set. We recall that a horizontal sum of a family of OMPs is obtained by taking their disjoint union and identifying their bottom and top elements 0 and 1.

**PROPOSITION 2.15.** *For  $X$  an 8-element set, the OMP FACT  $X$  is a horizontal sum of 30 copies of the OMP FACT  $\mathbb{Z}_2^3$ .*

**Proof.** Suppose we define an addition  $+$  and zero 0 on  $X$  so that that the resulting structure  $V = (X, +, 0)$  is a 3-dimensional vector space over  $\mathbb{Z}_2$ . Let FACT  $V$  be the set of all factor pairs  $(\theta_1, \theta_2)$  where  $\theta_1$  and  $\theta_2$  are congruences with respect to this vector space structure. Then FACT  $V$  is a sub-OMP of FACT  $X$  and FACT  $V_+$  is isomorphic to the OMP FACT  $\mathbb{Z}_2^3$ .

We claim that FACT  $X$  is the horizontal sum of its subalgebras that arise as FACT  $V$  for some vector space structure  $V$  on  $X$ . To establish the claim, it is enough to show that each block of FACT  $X$  is contained in some subalgebra FACT  $V$ , and that any block of FACT  $X$  that contains an atom of some FACT  $V$  is contained in this subalgebra. Once this claim is established, it follows from the above counting arguments that there are 30 such horizontal summands.

For any block of FACT  $X$ , there is a corresponding factor triple  $(\theta_1, \theta_2, \theta_3)$ . Each  $X/\theta_i$  is a 2-element set, and choosing some way to put  $\mathbb{Z}_2$ -vector space structure on each of these 2-element sets and taking the product structure on  $X$ , we have  $(\theta_1, \theta_2, \theta_3)$  is a factor triple of  $V$ . Then the given block is a block of the subalgebra FACT  $V$ . Suppose some block  $B$  of FACT  $X$  has an atom  $a$  belonging to some FACT  $V$ . The above counting arguments show there are 3 blocks of FACT  $X$  that contain  $a$  and 3 blocks of FACT  $V$  that contain  $a$ . So the block  $B$  must be a block of FACT  $V$ .  $\square$

**Remark 2.16.** For any set  $X$  whose cardinality is a prime power  $p^k$ , we may consider subalgebras of FACT  $X$  of the form FACT  $V$  where  $V$  is some  $k$ -dimensional  $\mathbb{Z}_p$ -vector space structure on  $X$ . We call such subalgebras  $\mathbb{Z}_p$ -blocks. One can show

- (1) FACT  $X$  has  $\frac{(p^3 - 1)!}{(p^3 - 1)(p^3 - p)(p^3 - p^2)} \mathbb{Z}_p$ -blocks.
- (2) Each atom of FACT  $X$  is in  $\frac{(p^2 - 1)!(p - 2)!}{(p^2 - 1)(p^2 - p)} \mathbb{Z}_p$ -blocks.
- (3) Each block of FACT  $X$  is in  $(p - 2)! \mathbb{Z}_p$ -blocks.

When  $|X| = 27$ , each block of FACT  $X$  is in just one  $\mathbb{Z}_3$ -block and each atom is in 840  $\mathbb{Z}_3$ -blocks. So FACT  $X$  is no longer a horizontal sum as in the case of  $|X| = 8$ .

### 3. Automorphisms

In this section, we make some general remarks about the group homomorphism  $\Gamma: \text{AUT}(A) \rightarrow \text{AUT}(\text{FACT } A)$  in the case that  $A$  is a finite set, or a finite-dimensional vector space. We begin with a description of  $\Gamma$  when applied to FACT  $X$  for a set  $X$ .

**DEFINITION 3.1.** For a set  $X$ , and permutation  $\alpha$  of  $X$ , define for each relation  $\theta$  on  $X$  the relation  $\alpha\theta = \{(\alpha x, \alpha y) : (x, y) \in \theta\}$ . Then define  $\Gamma: \text{AUT}(X) \rightarrow \text{AUT}(\text{FACT } X)$  by setting  $\Gamma\alpha$  to be the map with  $(\Gamma\alpha)(\theta, \theta') = (\alpha\theta, \alpha\theta')$ .

**PROPOSITION 3.2.** *If  $X$  is a set whose cardinality is neither prime, nor equal to 4, then the map  $\Gamma$  is an embedding. Consequently, the phase group of  $X$  is trivial.*

Proof. In these circumstances, there are  $m, n$  with  $m \geq 2$  and  $n \geq 3$  with  $|X| = mn$ . This includes the infinite case if we allow  $n$  to be infinite, but our diagrams will indicate the finite case. Suppose  $\alpha$  is a permutation of  $X$  with  $\Gamma\alpha$  the identity on FACT  $X$ . Suppose also there is some  $a \in X$  with  $\alpha a \neq a$ . Then we can enumerate the elements of  $X$  as  $a_{ij}$  where  $i \leq m$  and  $j \leq n$  so that  $a = a_{11}$  and  $\alpha(a) = a_{12}$ .

$$\begin{matrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{matrix}$$

There is a factor pair  $(\theta_1, \theta_2)$  with blocks of  $\theta_1$  being rows in the above diagram and blocks of  $\theta_2$  being the columns. As  $\Gamma\alpha$  is the identity,  $\alpha\theta_1 = \theta_1$  and  $\alpha\theta_2 = \theta_2$ . So  $\alpha$  maps the elements of one row to those of another, and the elements of one column to those of another. Thus there are permutations  $\mu$  of  $\{1, \dots, m\}$  and  $\nu$  of  $\{1, \dots, n\}$  with  $\alpha(a_{ij}) = a_{\mu(i)\nu(j)}$  for each  $i, j$ . As  $\alpha(a_{11}) = a_{12}$  we have  $\mu(1) = 1$  and  $\nu(1) = 2$ .

Swap places of  $a_{11}$  and  $a_{13}$  and consider next the factor pair  $(\phi_1, \phi_2)$  where the blocks of  $\phi_1$  are the rows of the diagram below, and the blocks of  $\phi_2$  are the columns.

$$\begin{matrix} a_{13} & a_{12} & a_{11} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{matrix}$$

Then  $\alpha(a_{12})$  belongs to the second column and  $\alpha(a_{13})$  does not. So  $\alpha\phi_2 \neq \phi_2$ , and this contradicts  $\Gamma\alpha$  being the identity. □

Let  $A$  be a structure with all blocks of FACT  $A$  finite. We say the automorphism group of FACT  $A$  is transitive on atoms if for any two atoms of FACT  $A$  there is an automorphism of FACT  $A$  mapping the first to the second. We say the automorphism group is transitive on blocks if for any two blocks of FACT  $A$  there is an automorphism of FACT  $A$  mapping the first block to the second. We say the automorphism group is strongly transitive on blocks if for any two blocks, and any two sequencings of the atoms of these blocks, there is an automorphism taking the first block to the second and compatible with the given sequencings. It is easily seen that strong transitivity on blocks implies transitivity on blocks, and this implies transitivity on atoms.

**PROPOSITION 3.3.** *For a finite set  $X$ , the automorphism group of FACT  $X$  is transitive on blocks. If  $|X|$  is a prime power, then it is strongly transitive on blocks.*

Proof. Here it is easiest to work with the definition of  $\Gamma$  from the introduction, where a permutation  $\alpha$  of  $X$  is taken to the automorphism  $\Gamma\alpha$  of FACT  $X$  that maps the equivalence class of the decomposition  $f: X \rightarrow Y \times Z$  to the equivalence class of the decomposition  $f \circ \alpha: X \rightarrow Y \times Z$ .

Given two blocks of FACT  $X$ , there are decompositions  $f: X \rightarrow Y_1 \times \dots \times Y_m$  and  $g: X \rightarrow Z_1 \times \dots \times Z_n$ , with each  $Y_i$  and  $Z_j$  directly irreducible, from which these blocks are built [13: Prop. 3.8]. In particular, the atoms of these blocks are of the equivalence classes of the binary decompositions

$$f_i: X \rightarrow Y_i \times \left( \prod_{j \neq i} Y_j \right) \quad \text{and} \quad g_i: X \rightarrow Z_i \times \left( \prod_{j \neq i} Z_j \right)$$

As each  $Y_i$  and  $Z_j$  are directly irreducible, they have prime cardinality, and the cardinality of  $X$  is the product of the cardinalities of the  $Y_i$ 's and of the  $Z_j$ 's. So  $m = n$ , and there exists a permutation  $\sigma$  of  $n$  and bijections  $h_i: Y_i \rightarrow Z_{\sigma(i)}$ .

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y_1 \times \cdots \times Y_n \\
 \alpha \uparrow & & \downarrow h_1 \qquad \qquad \downarrow h_n \\
 X & \xrightarrow{g_\sigma} & Z_{\sigma_1} \times \cdots \times Z_{\sigma_n}
 \end{array}$$

Denote  $g(x)$  by  $(g_1(x), \dots, g_n(x))$  and define  $g_\sigma(x) = (g_{\sigma_1}(x), \dots, g_{\sigma_n}(x))$ . Define a map  $k$  from  $Z_1 \times \cdots \times Z_n \rightarrow Y_1 \times \cdots \times Y_n$  by setting  $k(z_1, \dots, z_n) = (h_1^{-1}(z_{\sigma_1}), \dots, h_n^{-1}(z_{\sigma_n}))$ , and then let  $\alpha$  be the permutation of  $X$  given by  $\alpha = f^{-1} \circ k \circ g$ . Then for the usual product map  $h = h_1 \times \cdots \times h_n$ , we have the following for each  $x \in X$ .

$$\begin{aligned}
 (h \circ f \circ \alpha)(x) &= (h \circ f \circ f^{-1} \circ k \circ g)(x) \\
 &= (h \circ k)(g_1(x), \dots, g_n(x)) \\
 &= h(h_1^{-1}(g_{\sigma_1}(x)), \dots, h_n^{-1}(g_{\sigma_n}(x))) \\
 &= (h_1 h_1^{-1}(g_{\sigma_1}(x)), \dots, h_n h_n^{-1}(g_{\sigma_n}(x))) \\
 &= g_\sigma(x)
 \end{aligned}$$

Extending the definition of  $\Gamma\alpha$  to  $n$ -ary decompositions in the obvious way, we have that  $\Gamma\alpha$  takes the equivalence class of the decomposition  $f: X \rightarrow Y_1 \times \cdots \times Y_n$  to the equivalence class of the decomposition  $f \circ \alpha: X \rightarrow Y_1 \times \cdots \times Y_n$ . Then  $h_1, \dots, h_n$  are bijections showing that the  $n$ -ary decomposition  $f \circ \alpha: X \rightarrow Y_1 \times \cdots \times Y_n$  is equivalent to the  $n$ -ary decomposition  $g_\sigma: X \rightarrow Z_{\sigma_1} \times \cdots \times Z_{\sigma_n}$ . So  $\Gamma\alpha$  takes the equivalence class of  $f: X \rightarrow Y_1 \times \cdots \times Y_n$  to that of  $g_\sigma: X \rightarrow Z_{\sigma_1} \times \cdots \times Z_{\sigma_n}$ .

Consider the following binary decompositions.

$$f_i: X \rightarrow Y_i \times \left( \prod_{j \neq i} Y_j \right) \quad \text{and} \quad (g_\sigma)_i: X \rightarrow Z_{\sigma(i)} \times \left( \prod_{j \neq \sigma(i)} Z_j \right)$$

From the above remarks about  $\Gamma\alpha$  and its action with respect to  $f$  and  $g_\sigma$ , it follows that  $\Gamma\alpha$  maps the equivalence class of the first binary decomposition to the equivalence class of the second. Thus  $\Gamma\alpha$  maps the atoms of the first block to those of the second. Thus  $\Gamma$  is transitive on the blocks.

However, the sequencing of the matching of the atoms is determined by the permutation  $\sigma$ . If  $|X|$  is a prime power, then all irreducible factors have the same prime number of elements, and the permutation  $\sigma$  can be chosen to be the identity. In this case,  $\Gamma$  is strongly transitive on the blocks.  $\square$

The proof of the following result is nearly identical to the above.

**THEOREM 3.4.** *If  $V$  is a finite-dimensional vector space, then the automorphism group of FACT  $V$  is strongly transitive on blocks.*

**Remark 3.5.** In the setting of a structure  $A$  where the blocks of FACT  $A$  are all finite, the above proof shows that the automorphism group of FACT  $A$  is transitive on blocks iff a version of the Krüll-Schmidt theorem holds for  $A$ , namely, that any two direct product decompositions of  $A$  into irreducibles can be rearranged so that the factors are pairwise isomorphic. Likely there is a similar connection in the general setting, involving refinements of decompositions, but we have not pursued the matter.

We now turn our attention to the computation of the automorphism group, and behavior of  $\Gamma$  for some “small” sets  $X$ . We recall that the phase group of a structure is the kernel of the map  $\Gamma$ .

**PROPOSITION 3.6.** *Suppose  $X$  is a set of prime cardinality  $p$ . Then  $\text{FACT } X$  has 2 elements, its automorphism group is trivial,  $\Gamma$  is onto, and the phase group of  $X$  is the full symmetric group on  $X$ .*

**PROOF.** This is obvious from the fact that a set with a prime number of elements can only be decomposed as a direct product as a one-element set times a  $p$ -element set, or as a  $p$ -element set times a one-element set, and any two decompositions of either type are equivalent.  $\square$

Recall that the orthomodular poset  $\text{MO}_n$  is a horizontal sum of  $n$  copies of the 4-element Boolean algebra. So it has a bottom, a top, and an antichain of  $2n$  elements in the middle paired as orthocomplements. We shall also use the following simple observation.

**LEMMA 3.7.** *If  $L$  is the horizontal sum of  $k$  copies of the OMP  $P$ , then  $\text{AUT } L$  is the semidirect product  $(\text{AUT } P)^k \rtimes \text{SYM}(k)$  of the  $k^{\text{th}}$  power of the automorphism group of  $P$  by the symmetric group on  $k$  letters via the obvious action.*

We consider next our first somewhat anomalous case, that where  $|X| = 4$ . We note that this is a prime power of 2. The next prime power of 2, when  $|X| = 8$ , will also provide unusual behavior. Somehow it seems there is just insufficient room in factors of 2 to behave properly. We do not know what happens when  $|X| = 2^4$ .

**PROPOSITION 3.8.** *If  $X$  has cardinality 4, then  $\text{FACT } X$  is  $\text{MO}_3$ , its automorphism group is  $(\mathbb{Z}_2)^3 \rtimes \text{SYM}(3)$ , its phase groups is the Klein four group, and  $\Gamma$  is not onto.*

**PROOF.** As  $|X|$  has two prime factors, all blocks have two atoms, so it is an  $\text{MO}_n$  for some  $n$ . It follows from either Corollary 2.3 or 2.4 that  $\text{FACT } X$  has 6 atoms, hence is  $\text{MO}_3$ . Lemma 3.7 then describes the automorphism group of  $\text{FACT } X$  since the automorphism group of a 4-element Boolean algebra is  $\mathbb{Z}_2$ . That  $\Gamma$  is not onto follows as  $\text{AUT}(X)$  has  $4!$  elements, so is smaller than that of  $\text{FACT } X$ . It remains only to observe that the kernel of  $\Gamma$  is the Klein four group. For this, one computes directly that if  $X = \{a, b, c, d\}$ , then the permutations  $\alpha$  of  $X$  with  $\Gamma\alpha = \text{id}$  are  $\text{id}$ , and the ones whose cycle representations are  $(ab)(cd)$ ,  $(ac)(bd)$ , and  $(ad)(bc)$ .  $\square$

**PROPOSITION 3.9.** *If  $|X| = pq$  with  $p, q$  prime and  $p \geq 3$ , then  $\text{FACT } X$  is  $\text{MO}_n$  where*

$$n = \begin{cases} \frac{(pq)!}{p!q!} & \text{if } p \neq q \\ \frac{(pq)!}{2p!q!} & \text{if } p = q \end{cases}$$

*The automorphism group of  $\text{FACT } X$  is  $(\mathbb{Z}_2)^n \rtimes \text{SYM}(n)$ , the phase group is trivial, and  $\Gamma$  is not onto.*

**PROOF.** As  $|X|$  has two prime factors, its blocks are 4-element Boolean algebras, so it is an  $\text{MO}_n$  where  $n$  is the number of blocks. When  $p \neq q$ , the number of blocks equals the number of factor pairs  $(\theta_1, \theta_2)$  where  $\theta_1$  has  $p$  blocks of  $q$  elements each, as each block contains one such factor pair. By Corollary 2.3 the number of blocks is as given above. When  $p = q$  each block contains two factor pairs  $(\theta_1, \theta_2)$  where  $\theta_1$  has  $p$  blocks of  $p$  elements each, and is half the number of atoms. This is given by either of Corollary 2.3 or 2.4 to be as above. The description of the automorphism group is given by Lemma 3.7 as the automorphism groups of the blocks are  $\mathbb{Z}_2$ . Proposition 3.2 shows the phase group is trivial, and as the automorphism group of  $\text{FACT } X$  has much larger cardinality than that of  $X$ ,  $\Gamma$  is not onto.  $\square$

**PROPOSITION 3.10.** *If  $|X| = 8$ , then FACT  $X$  is a horizontal sum of 30 copies of FACT  $\mathbb{Z}_2^3$ , its automorphism group is  $(\text{AUT}(\text{FACT } \mathbb{Z}_2^3))^{30} \rtimes \text{SYM}(30)$ . The phase group is trivial, and  $\Gamma$  is not onto.*

*Proof.* The description of FACT  $X$  in this case is given in Proposition 2.15, and the description of its automorphism group then follows from Lemma 3.7. Proposition 3.2 shows the phase group is trivial, and as the automorphism group of FACT  $X$  has much larger cardinality than that of  $X$ ,  $\Gamma$  is not onto.  $\square$

The result above is incomplete since it describes matters in terms of the group  $\text{AUT}(\text{FACT } \mathbb{Z}_2^3)$ . However, in a nice series of papers [7–9, 27], results are given that in conjunction with the fundamental theorem of projective geometry describe the automorphism group of FACT  $V$  for any finite-dimensional vector space  $V$ . We briefly describe these results below. First, we note SUB  $V$  is used to denote the subspace lattice of  $V$ , by a dual automorphism of SUB  $V$  we mean an isomorphism from this lattice to its dual lattice.

**THEOREM 3.11.** ([9]) *For a finite-dimensional vector space  $V$ , each automorphism  $\sigma$  and dual automorphism  $\mu$  of SUB  $V$  give automorphisms  $\sigma^*$  and  $\mu^*$  of FACT  $V$  where*

$$\sigma^*(S, T) = (\sigma S, \sigma T) \quad \text{and} \quad \mu^*(S, T) = (\mu T, \mu S).$$

*Further, each automorphism of FACT  $V$  arises this way.*

It is worthwhile to briefly describe the proof of this result as it illuminates the proof in the following section. The key step is the following. Here, an element of FACT  $V$  is said to be of height two if it covers an atom.

**LEMMA 3.12.** *Two atoms of FACT  $V$  have at least two distinct upper bounds of height two iff they have the same first components or the same second components.*

The proof is not difficult, relying on a bit of elementary modular lattice theory. With this result, there is a foothold on automorphisms of FACT  $V$  as two atoms satisfying this condition must be mapped to two others satisfying it. Thus two atoms with the same first coordinate either get mapped to two with the same first coordinate, or two with the same second coordinate. With some work, one shows that an automorphism  $\phi$  of FACT  $V$  either takes all pairs with the same first coordinate to ones with the same first coordinate, or to ones with the same second coordinate. From this, it is not difficult to show that  $\phi$  equal to  $\alpha^*$  for some automorphism  $\alpha$  of SUB  $V$  in the first case, and equal to  $\delta^*$  for some anti-automorphism of SUB  $V$  in the second.

**THEOREM 3.13 (The Fundamental Theorem of Projective Geometry I).** ([3]) *For a finite-dimensional vector space  $V$ , the automorphisms of SUB  $V$  correspond to the collineations of the projective geometry associated with  $V$ . Each semi-linear automorphism of  $V$  gives an automorphism of SUB  $V$ , all automorphisms of SUB  $V$  arise this way, and two semi-linear automorphisms give the same automorphism of SUB  $V$  iff they are scalar multiples of one another.*

We next introduce notation for various groups of automorphisms.

**DEFINITION 3.14.** For a finite-dimensional vector space  $V$  over a field  $\mathfrak{K}$ , denote the groups of linear automorphisms, semilinear automorphisms, and automorphisms that are scalar multiples by  $\text{GL}(V)$ ,  $\text{SL}(V)$  and  $\mathfrak{K}^*$  respectively. Then let  $\text{PGL}(V)$  and  $\text{PSL}(V)$  be the quotients of  $\text{GL}(V)$  and  $\text{SL}(V)$  by  $\mathfrak{K}^*$ .

Note  $\text{GL}(V)$  is by definition the automorphism group of  $V$ , and the fundamental theorem of projective geometry states  $\text{PSL}(V)$  is the automorphism group of SUB  $V$ . Clearly  $\text{PSL}(V)$  is a subgroup of index 2 in the group of all automorphisms and dual automorphisms of SUB  $V$ , and

by Chevalier’s result, Theorem 3.11, this is the automorphism group of FACT  $V$ . This gives the following.

**THEOREM 3.15.** *Let  $V$  be a finite-dimensional vector space over a field  $\mathfrak{K}$ . The phase group of  $V$  is the group  $\mathfrak{K}^*$  of non-zero elements of  $\mathfrak{K}$ . The image of  $\Gamma$  is  $\text{PGL}(V)$ , and this is a subgroup of the index 2 subgroup  $\text{PSL}(V)$  of  $\text{AUT}(\text{FACT } V)$ . If  $\mathfrak{K}$  has no non-trivial automorphisms, then  $\text{PGL}(V) = \text{PSL}(V)$ , so the image of  $\Gamma$  has index 2 in the automorphism group of FACT  $V$ .*

#### 4. The case of a 27-element set — the first half

We show that for  $X$  a 27-element set, the map  $\Gamma$  gives an isomorphism from the permutation group of  $X$  to the group of automorphisms of FACT  $X$ . The proof has two main parts. The first is to show that the automorphisms of FACT  $X$  correspond to automorphisms of the poset  $\text{REQ } X$  of regular equivalence relations of  $X$ , i.e. those equivalence relations where every block has the same size. That is the content of this section. The second half is to show that automorphisms of  $\text{REQ } X$  correspond to permutations of  $X$ , and is in the following section.

**NOTATION 4.1.** An equivalence relation on  $X$  with 9 blocks of 3 elements each is called a small relation, and usually denoted by a lower case latin letter such as  $a$ . Its blocks are denoted  $a_1, \dots, a_9$ . An equivalence relation with 3 blocks of 9 elements each is called a large relation and denoted by an upper case latin letter such as  $A$ . Its blocks are denoted  $A_1, \dots, A_3$ . Ordered pairs of equivalence relations, such as  $(a, A)$ , will be written as  $aA$ .

We review some basics from Section 1 in this setting. The blocks of FACT  $X$  all have 3 atoms, and each element of FACT  $X$  is either a bound 0 or 1, an atom, or a coatom. The non-trivial factor pairs of  $X$  are the  $aA$  and  $Aa$  where  $a$  is small,  $A$  is large, and  $a \cap A = \Delta$  where  $\Delta$  is the identity relation. Of these, the  $aA$  are the atoms and the  $Aa$  are the coatoms of FACT  $X$ . For atoms  $aA$  and  $bB$  we have  $aA \perp bB$  iff  $a \subseteq B$ ,  $b \subseteq A$ , and  $a, b$  permute. We come to our key notion that will allow us to deal with automorphisms of FACT  $X$ .

**DEFINITION 4.2.** Call sets of atoms  $\mathfrak{X}$  and  $\mathfrak{Y}$  of FACT  $X$  orthogonal, and write  $\mathfrak{X} \perp \mathfrak{Y}$  if each member of  $\mathfrak{X}$  is orthogonal to each member of  $\mathfrak{Y}$ .

We next turn to the results on orthogonal sets of atoms that will allow us to show that automorphisms of FACT  $X$  act component-wise on factor pairs. In its proof, and elsewhere, we assume  $X$  is the set  $\{0, 1, 2\}^3$ . We frequently draw  $X$  as shown below, and use suggestive terminology such as the bottom floor, middle floor, top floor, left side wall, middle wall, right wall, front wall, back wall, in the obvious way. We refer to the elements of  $X$  as strings such as 102 rather than as ordered triples  $(1, 0, 2)$  to aid readability of diagrams. The  $x, y, z$ -axes have their usual meaning.

**PROPOSITION 4.3.** *Suppose  $a, b$  are small, permute, and have  $a \cap b = \Delta$ . Set*

$$\begin{aligned} \mathfrak{X}(a, b) &= \{aA : aA \text{ is an atom and } b \subseteq A\} \\ \mathfrak{Y}(a, b) &= \{bB : bB \text{ is an atom and } a \subseteq B\} \end{aligned}$$

*Then  $\mathfrak{X}(a, b)$  and  $\mathfrak{Y}(a, b)$  each have 36 elements and  $\mathfrak{X}(a, b) \perp \mathfrak{Y}(a, b)$ . Further, the intersection of the second coordinates,  $A$ , of members of  $\mathfrak{X}(a, b)$  is  $b$ , and the intersection of the second coordinates,  $B$ , of members of  $\mathfrak{Y}(a, b)$  is  $a$ .*

**PROOF.** Assume blocks of  $a$  are lines parallel to the  $z$ -axis, and blocks of  $b$  are lines parallel to the  $y$ -axis. As  $a, b$  are small, permute, and  $a \cap b = \Delta$  we have  $a \circ b$  is an equivalence relation that must

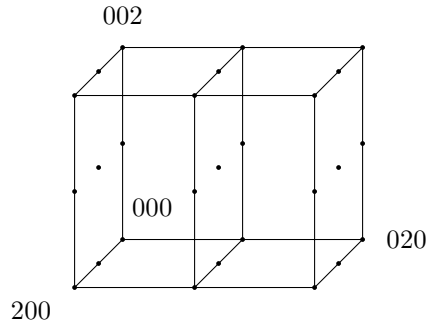


FIGURE 1.  $X$

be large, in this case its blocks are the planes  $x = 0$ ,  $x = 1$  and  $x = 2$ , i.e. the front wall, middle wall, and back wall. It follows that this assumption on the choice of  $a, b$  general.

The large  $A$  with  $aA \in \mathfrak{X}(a, b)$  are those with  $b \subseteq A$  and  $a \cap A = \Delta$ . These conditions mean that each block of  $A$  consists of 3 lines in the  $y$ -direction ( $b$ -blocks) and that no two of these lines are vertical translates of one another (since  $A \cap a = \Delta$ ). So each of the blocks of  $A$  contains exactly one of 000, 001, and 002.

The block of  $A$  containing 000 must contain the line in  $y$ -direction with 000, as well as one line  $y$ -direction from the plane  $x = 1$ , and one line  $y$ -direction from the plane  $x = 2$ . So there are  $3 \cdot 3$  ways to construct this block of  $A$ . Assuming the block containing 000 is chosen, we consider the block of  $A$  containing 001. This block contains the line  $y$ -direction with 001 as well as one of the two remaining lines  $y$ -direction from the plane  $x = 1$ , and one of the two remaining lines  $y$ -direction from the plane  $x = 2$ . So there are  $2 \cdot 2$  ways to construct this block. Then the final block of  $A$  is determined. In all, there are  $3 \cdot 3 \cdot 2 \cdot 2 = 36$  ways to construct  $A$ .

We have shown that  $\mathfrak{X}(a, b)$  has 36 elements, and by symmetry so does  $\mathcal{Y}(a, b)$ . To see  $\mathfrak{X}(a, b) \perp \mathcal{Y}(a, b)$  suppose  $aA \in \mathfrak{X}(a, b)$  and  $bB \in \mathcal{Y}(a, b)$ . By definition  $a \subseteq B$ ,  $b \subseteq A$ , and we began by assuming  $a, b$  permute. Thus  $aA \perp bB$ . The description of the large  $A$  with  $aA \in \mathfrak{X}(a, b)$  shows their intersection is  $b$ , and this, with its dual statement, gives the further condition of the proposition.  $\square$

We next show that these simple conditions characterize the sets arising as  $\mathfrak{X}(a, b)$  and  $\mathcal{Y}(a, b)$ . This proof will take some effort and is spread through a number of claims across several pages.

**PROPOSITION 4.4.** *If  $\mathfrak{X}, \mathcal{Y}$  are two sets of 36 atoms each with  $\mathfrak{X} \perp \mathcal{Y}$ , then there are small permuting  $a, b$  with  $a \cap b = \Delta$  such that  $\mathfrak{X} = \mathfrak{X}(a, b)$  and  $\mathcal{Y} = \mathcal{Y}(a, b)$ .*

**PROOF.** Suppose the atoms in  $\mathfrak{X}$  are  $x_i X_i$  and those in  $\mathcal{Y}$  are  $y_j Y_j$  for  $i, j = 1, \dots, 36$ . We assume further that  $x_1 X_1$  is the factor pair where the  $x_1$  blocks are lines parallel to the  $z$ -axis and the  $X_1$  blocks are the planes  $z = 0, z = 1, z = 2$ ; and  $y_1 Y_1$  is the factor pair where the  $y_1$  blocks are the lines parallel to the  $y$ -axis and  $Y_1$  blocks are the planes  $y = 0, y = 1, y = 2$ .

**CLAIM 4.5.** *There are 36 small  $u$  with  $uY_1$  an atom orthogonal to  $x_1 X_1$ , and the transitive closure of the union of these  $u$ 's is  $X_1$ .*

**PROOF.** Such  $u$  must be small, permute with  $x_1$ , be contained in  $X_1$  and intersect  $Y_1$  trivially. As  $u$  is contained in  $X_1$  it partitions each block of  $X_1$  (the planes  $z = 0, 1, 2$ ) into three pieces of three, and as  $u$  permutes with  $x_1$  (whose blocks are vertical lines), the partitions of these three planes must be vertical translates of one another. So  $u$  is completely determined by its intersection with the plane  $z = 0$ . As  $u$  intersects  $Y_1$  trivially, none of the blocks of  $u$  in the plane  $z = 0$  contains



AUTOMORPHISMS OF DECOMPOSITIONS

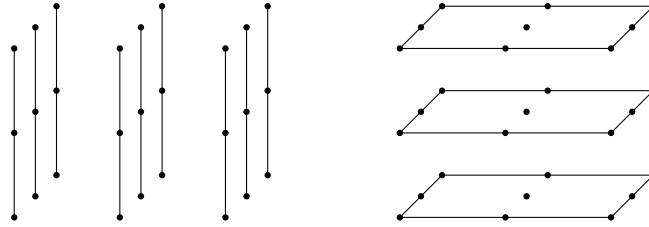


FIGURE 2.  $x_1$  and  $X_1$

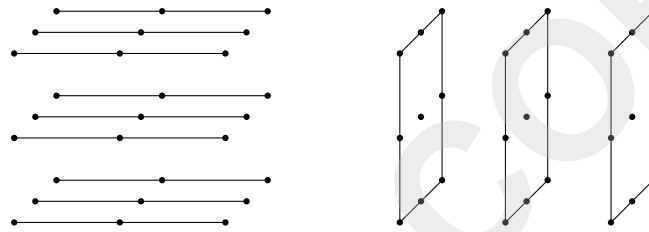


FIGURE 3.  $y_1$  and  $Y_1$

two elements with the same  $y$ -coordinate. So each of these three blocks contains exactly one of 000, 100, 200. There are  $3 \cdot 3$  ways to choose the block containing 000, then  $2 \cdot 2$  ways to choose the block containing 100. This then determines  $u$ , so there are 36 such  $u$ . It is clear from the description of the construction of such  $u$ 's that the transitive closure of their union is  $X_1$ .  $\square$

**CLAIM 4.6.** *It cannot happen that all  $x_i X_i$  or all  $y_j Y_j$  have the same second coordinate.*

**Proof.** Suppose all the  $y_j Y_j$  have the same second coordinate, which will be  $Y_1$ . As each  $y_j Y_j$  is an atom orthogonal to  $x_1 X_1$ , the  $y_j$  for  $j = 1, \dots, 36$  must be the 36  $u$ 's of Claim 4.5. Since  $x_i X_i \perp y_j Y_j$  for each  $i, j$ , we have  $y_j \subseteq X_i$  for each  $i, j$ , and as the  $y_j$  are the 36  $u$ 's, and the transitive closure of these 36  $u$ 's is  $X_1$ , it follows that  $X_i = X_1$  for each  $i$ . Using a symmetric version of Claim 4.5, there are 36 small  $v$ 's with  $v X_1$  an atom orthogonal to  $y_1 Y_1$ , and these  $v$ 's must be the  $x_i$ . These  $v$ 's are the small congruences that partition blocks of  $Y_1$  (the planes  $y = 0, 1, 2$ ) into blocks of three, are disjoint from  $X_1$ , and whose partitions of the different blocks of  $Y_1$  are translates of one another along the  $y$ -axis. One such choice of  $u, v$  is shown below.

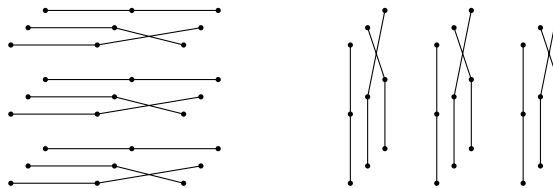


FIGURE 4. A choice of  $u$  and  $v$

Note that the transitive closure of the union of the blocks of  $u, v$  containing 200 has more than 9 elements, and as  $u \cap v = \Delta$ , this implies they do not permute. This provides a contradiction to the fact that  $x_i X_i \perp y_j Y_j$ , since this implies  $x_i$  permutes with  $y_j$  for each  $i, j$ .  $\square$

If all the  $x_i X_i$  have the same first component, they must all have different second components, and these second components must all contain  $y_1$ . This implies that  $\mathfrak{X}$  is contained in  $\mathfrak{X}(x_1, y_1)$  and as both have 36 elements, they are equal. Proposition 4.3 gives that the intersection of the second members of  $\mathfrak{X}(x_1, y_1)$  equals  $y_1$ . As this intersection contains each  $y_j$ , this implies that all  $y_j Y_j$  have the same first component, hence  $\mathcal{Y} = \mathcal{Y}(x_1, y_1)$ . This would establish our result, as would the dual argument if all  $y_j Y_j$  have the same first components. Modulo a renumbering of the elements, we then have the following result that we will use to argue by contradiction.

**CLAIM 4.7.** *If Proposition 4.4 is not true, then  $x_1 \neq x_2$  and  $y_1 \neq y_2$ .*

Since we have  $x_i X_i \perp y_1 Y_1$ , the blocks of  $x_i$  are contained in the blocks of  $Y_1$  (the planes  $y = 0, 1, 2$ ) and the blocks of  $x_i$  contained in one of these planes are translates in the  $y$ -direction (since blocks of  $y_1$  are lines in the  $y$ -direction) of the blocks contained in another plane. Similarly, the blocks of  $y_j$  are contained in the blocks of  $X_1$  (the planes  $z = 0, 1, 2$ ) and the blocks of  $y_j$  contained in one of these planes are translates in the  $z$ -direction (since blocks of  $x_1$  are lines in the  $z$ -direction) of the blocks contained in another plane.

**CLAIM 4.8.** *If  $x_i \neq x_1$  and  $y_j \neq y_1$ , then the transitive closures  $\text{TRCL}(x_1 \cup x_i)$  and  $\text{TRCL}(y_1 \cup y_2)$  each have three blocks of three and three blocks of six.*

*Proof.* We know  $x_1 \neq x_i$ , both are contained in  $Y_1$ , and both are determined by their intersection with one of the blocks (planes) of  $Y_1$ . So  $\text{TRCL}(x_1 \cup x_i)$  is also determined by its intersection with one block of  $Y_1$ . As the transitive closure coalesces blocks of  $x_1$ , this intersection with a block of  $Y_1$  can have

- (i) three blocks of three,
- (ii) one block of three and one block of six, or
- (iii) one block of nine.

The first case gives  $x_1 = x_i$ . The third implies the transitive closure is  $Y_1$ . As  $x_1, x_i \subseteq Y_j$  for each  $j$ , we would then have  $Y_1 = Y_j$  for all  $j$ , contrary to Claim 5.19. So if  $x_1 \neq x_i$ , the second case must hold. The argument for  $y_1 \neq y_j$  is similar.  $\square$

By Claim 5.19 each  $y_j$  must contain a block of  $y_1$  that is contained in the plane  $z = 0$ , hence must contain one of the lines in the  $y$ -direction containing 000, 100 or 200. There is symmetry to the situation, and we make the following assumption.

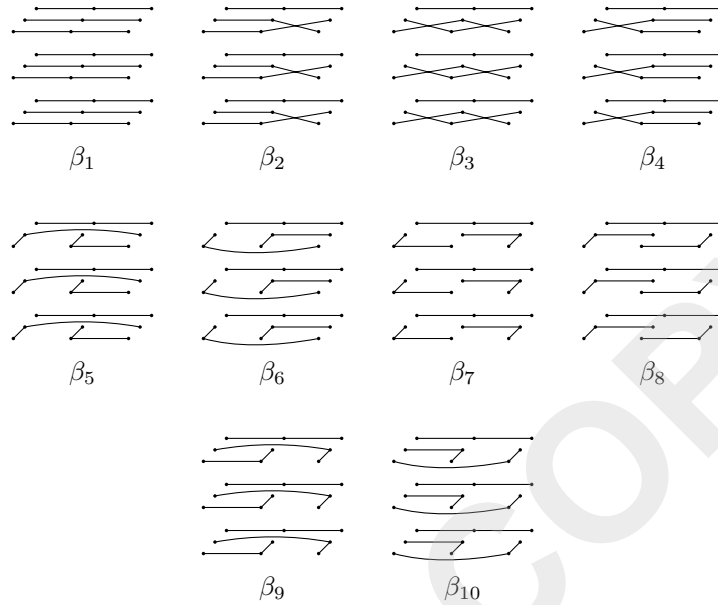
**ASSUMPTION 4.9.** The relation  $y_2$  contains 000, 010, 020.

Consider the small relations  $\beta$  that are contained in  $X_1$ , permute with  $x_1$ , and contain the block 000, 010, 020. As such  $\beta$  are determined by their intersection with the block (plane)  $z = 0$  of  $X_1$ , they partition the remaining six elements of this plane into two blocks of three. There are ten ways to do this, shown below as  $\beta_1, \dots, \beta_{10}$  with  $\beta_1 = y_1$ . The discussion above provides the following claim.

**CLAIM 4.10.** *The relation  $y_2$ , and any other  $y_j$  that also contains the block 000, 010, 020, is one of  $\beta_1, \dots, \beta_{10}$ .*

For any  $i$  we have  $x_i \subseteq Y_1$ , that  $x_i$  permutes with  $y_1, y_2$ , and if  $x_1 \neq x_i$  then  $\text{TRCL}(x_1 \cup x_i)$  has three blocks of three and three blocks of six. So the blocks of  $x_i$  are contained in the blocks

AUTOMORPHISMS OF DECOMPOSITIONS



(planes) of  $Y_1$ , and as  $x_i$  permutes with  $y_1$ , the blocks of  $x_i$  in one plane of  $Y_1$  are translates in the  $y$ -direction of the blocks of  $x_i$  in another plane of  $Y_1$ . So  $x_i$  is determined by its intersection with the plane  $y = 0$ , and the description of  $\text{TRCL}(x_1 \cup x_i)$  shows  $x_i$  contains one of the blocks of  $x_1$  in this plane.

**CLAIM 4.11.** *Under Assumption 4.9, all the  $x_i$  contain 000, 001, 002.*

*Proof.* We know each  $x_i$  contains a block of  $x_1$  in the plane  $y = 0$ . Suppose this is the block is the vertical line above 200. As  $x_i$  permutes with  $y_1$ , it also contains the vertical lines above 210 and above 220. If  $x_i \neq x_1$ , then as  $x_i$  is determined by its intersection with the plane  $y = 0$ , there are  $u, v$  with  $x_i$  relating  $00u$  and  $10v$ . As the blocks of  $x_i$  in the planes  $y = 1, y = 2$  are translates in the  $y$ -direction of its blocks in the plane  $y = 0$ ,  $x_i$  relates  $0mu$  and  $1mv$  for  $m = 0, 1, 2$ .

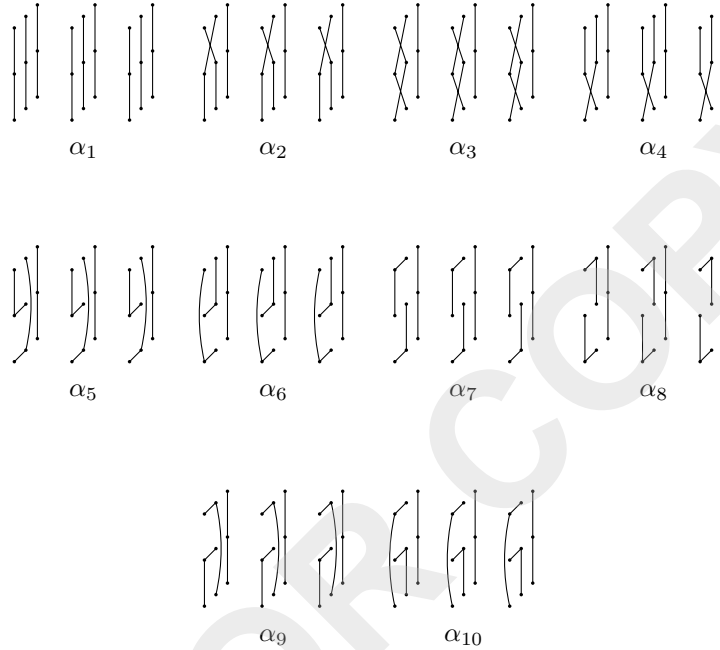
We know  $y_2$  is one of  $\beta_2, \dots, \beta_{10}$ . Inspecting these  $\beta_j$  there are some  $a, b$  with  $y_2$  relating  $1a0$  and  $2b0$ . Let  $cd0$  be the third point in this block of  $y_2$ . Consider the equivalence class  $S$  of  $\text{TRCL}(x_i \cup y_2)$  that contains  $2b0$ . As the vertical line above  $2b0$  is a block of  $x_i$ , and  $\{1an, 2bn, cdn\}$  is a block of  $y_2$  for each  $n = 0, 1, 2$ , the class  $S$  contains the nine elements  $\{1an, 2bn, cdn : n = 0, 1, 2\}$ .

Setting  $m = a$  shows  $x_i$  relates  $0au$  and  $1av$ . But  $1av$  belongs to  $\text{TRCL}(x_i \cup y_2)$ , hence so does  $0au$ . This shows  $S$  has more than 9 elements, and this implies  $x_i$  does not permute with  $y_2$ , a contradiction. Thus if  $x_i$  contains the vertical line above 200 it must be  $x_1$ , and a similar argument shows that if  $x_i$  contains the vertical line above 100 it is  $x_1$ . Therefore, if  $x_i \neq x_1$  it must contain the vertical line above 000. □

**CLAIM 4.12.** *Under Assumption 4.9, all the  $y_j$  contain the block 000, 010, 020, hence all are among  $\beta_1, \dots, \beta_{10}$ .*

*Proof.* By Claim 4.8, each  $y_j$  contains a line in the  $y$ -direction containing either 000, 100 or 200. The arguments in Claim 4.11 show that if  $y_2$  contains the line with 000, then all the  $x_i$  contain the vertical line with 000. Symmetry clearly shows that if  $y_2$  contains the horizontal line with  $n00$ , then all  $x_i$  contain the vertical line with  $n00$ . In any case, all  $x_i \neq x_1$  contain the same vertical line. Clearly the dual argument shows all  $y_j \neq y_1$  contain the same horizontal line. □

There are ten small  $\alpha$  that are contained in  $Y_1$ , permute with  $y_1$ , and contain the block 000,001,002. These shown below as  $\alpha_1, \dots, \alpha_{10}$  with  $\alpha_1 = x_1$ . The above results show all the  $x_i$  are among  $\alpha_1, \dots, \alpha_{10}$ , and all the  $y_j$  are among  $\beta_1, \dots, \beta_{10}$ .

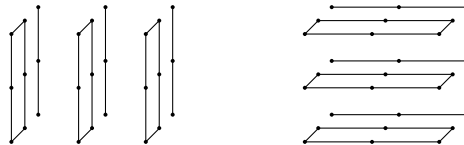


**CLAIM 4.13.** *The  $x_i$  are among  $\alpha_1, \dots, \alpha_4$  and the  $y_j$  are among  $\beta_1, \dots, \beta_4$ .*

**Proof.** If we consider  $\text{TRCL}(\alpha_i \cup \beta_j)$  for  $i = 5, \dots, 10$  and  $j = 2, \dots, 4$  we see that the block containing 200 consists of all elements in the planes  $x = 1, x = 2$ . It follows that  $\alpha_i$  does not permute with  $\beta_j$ . If we consider  $\text{TRCL}(\alpha_i \cup \beta_j)$  for  $i = 2, \dots, 4$  and  $j = 5, \dots, 10$  we see that the block containing 200 again consists of all elements in the planes  $x = 1, x = 2$ . So in this case also  $\alpha_i$  does not permute with  $\beta_j$ . Note also that  $\alpha_i \cap \beta_j \neq \Delta$  when  $i = 5, \dots, 10$  and  $j = 5, \dots, 10$ . So if some  $x_i$  is one of  $\alpha_5, \dots, \alpha_{10}$ , then no  $y_j$  can be one of  $\beta_2, \dots, \beta_{10}$  since for each  $x_i$  and  $y_j$  we have  $x_i$  permutes with  $y_j$  and  $x_i \cap y_j = \Delta$ . But this is contrary to some  $y_j \neq y_1$ , so no  $x_i$  can be among  $\alpha_5, \dots, \alpha_{10}$ . Similarly no  $y_j$  can be among  $\beta_5, \dots, \beta_{10}$ .  $\square$

**CLAIM 4.14.** *Each of  $\mathfrak{X}$  and  $\mathfrak{Y}$  have at most 24 elements.*

**Proof.** By Claim 4.13 we have  $x_2 = \alpha_i$  and  $y_2 = \beta_j$  for some  $i, j = 2, 3, 4$ . The the diagram below shows  $\text{TRCL}(x_1 \cup x_2)$  and  $\text{TRCL}(y_1 \cup y_2)$ .



Each  $Y_j$  contains  $\text{TRCL}(x_1 \cup x_2)$  and each  $X_i$  contains  $\text{TRCL}(y_1 \cup y_2)$ . To find a large relation that contains  $\text{TRCL}(x_1 \cup x_2)$  we must pair the three vertical lines with the three blocks of six. So

there are six ways to construct a large relation containing  $\text{TRCL}(x_1 \cup x_2)$ , and similarly six large relations containing  $\text{TRCL}(y_1 \cup y_2)$ . So there are at most six different  $X_i$  and at most six different  $Y_j$ . As there are at most four choices for  $x_i$  and four for the  $y_j$  our claim is proved.  $\square$

This contradiction proves Proposition 4.4.  $\square$

We now begin the task of using Proposition 4.4 to work with automorphisms. For this, a different method of representing  $X$  is convenient for a number of the proofs. We assume the elements of  $X$  are  $1, \dots, 27$  and indicate a factor pair  $aA$  of  $X$  by arranging the numbers  $1, \dots, 27$  in three columns of 9 elements each, with the rows of the array being the blocks of the small relation  $a$ , and the columns of the array being the blocks of the large relation  $A$ .

1	10	19
2	11	20
3	12	21
4	13	22
5	14	23
6	15	24
7	16	25
8	17	26
9	18	27

**DEFINITION 4.15.** Atoms  $aA$  and  $aB$  with the same first coordinate are near to one another if  $A \cap B$  has one block of 9 elements, 2 blocks of 6 elements, and 2 blocks of 3 elements.

Note that  $aA$  and  $aB$  are near if  $aB$  is obtained by picking three elements  $x_1, x_2, x_3$  in a block  $A_1$  of  $A$ , picking a second block  $A_2$  of  $A$ , finding the three elements  $y_1, y_2, y_3$  in  $A_2$  with  $x_i$  and  $y_i$  related by  $a$ , and then constructing  $B$  by *switching*  $x_1, x_2, x_3$  and  $y_1, y_2, y_3$ . More precisely, let  $B_1 = A_1 - \{x_1, x_2, x_3\} \cup \{y_1, y_2, y_3\}$ ,  $B_2 = A_2 - \{y_1, y_2, y_3\} \cup \{x_1, x_2, x_3\}$ , and  $B_3 = A_3$ . Below is an example of two atoms near to one another. The bullet marks indicate the rows of the elements involved in the *switching*.

•	1	10	19	10	1	19
•	2	11	20	11	2	20
•	3	12	21	12	3	21
	4	13	22	4	13	22
	5	14	23	5	14	23
	6	15	24	6	15	24
	7	16	25	7	16	25
	8	17	26	8	17	26
	9	18	27	9	18	27

**LEMMA 4.16.** If  $aA$  and  $aB$  are near, there is a small  $d$  with  $aA$  and  $aB$  in  $\mathfrak{X}(a, d)$ .

*Proof.* Up to relabeling of elements of  $X$ , the situation shown above is typical. Let  $d$  be the small relation whose blocks are obtained by splitting each column into three batches of three so that the swapped elements form two blocks. For instance,  $d$  might be  $\{1, 2, 3\}$ ,  $\{4, 5, 6\}$ ,  $\{7, 8, 9\}$ ,  $\{10, 11, 12\}$ ,  $\{13, 14, 15\}$ ,  $\{16, 17, 18\}$ ,  $\{19, 20, 21\}$ ,  $\{22, 23, 24\}$ ,  $\{25, 26, 27\}$ .  $\square$

**PROPOSITION 4.17.** If  $aA$  and  $aB$  are atoms with the same first coordinate, then their images under an automorphism  $\Phi$  of  $\text{FACT } X$  also have the same first coordinate.

*Proof.* Note first that any  $\mathfrak{X}(a, d)$  and  $\mathfrak{Y}(a, d)$  are two sets of 36 atoms each with  $\mathfrak{X}(a, d) \perp \mathfrak{Y}(a, d)$ . Therefore the same is true of the images of these sets under  $\Phi$ , so Proposition 4.4 says the images of these sets are of the form  $\mathfrak{X}(a', d')$  and  $\mathfrak{Y}(a', d')$  for some  $a', d'$ . So if  $aA$  and  $aA'$  are two atoms that belong to some  $\mathfrak{X}(a, d)$ , then the images of  $aA$  and  $aA'$  under  $\Phi$  must have the same first coordinate. In particular, if  $aA$  and  $aA'$  are near, their images have the same first coordinate.

**CLAIM 4.18.** *If  $aA$  and  $aB$  are atoms and  $B$  is formed from  $A$  by swapping two elements that lie in the same block of  $a$ , then the images of  $aA$  and  $aB$  under  $\Phi$  have the same first coordinate.*

*Proof.* Up to relabeling the elements of  $X$ , we may assume  $aA$  is the factor pair discussed above and that  $B$  is formed from  $A$  by swapping the elements 1, 10. In the figure below, we have six factor pairs  $aA_0, \dots, aA_5$  with  $A_0 = A$  and  $A_5 = B$ .

1	10	19	1	10	19	• 1	10	19
2	11	20	2	11	20	• 2	11	20
3	12	21	3	12	21	3	12	21
4	13	22	• 4	13	22	13	4	22
5	14	23	• 5	14	23	14	5	23
6	15	24	• 6	15	24	15	6	24
• 7	16	25	16	7	25	• 16	7	25
• 8	17	26	17	8	26	17	8	26
• 9	18	27	18	9	27	18	9	27

10	1	19	10	1	19	10	1	19
11	2	20	• 11	2	20	2	11	20
3	12	21	3	12	21	3	12	21
13	4	22	• 13	4	22	4	13	22
• 14	5	23	5	14	23	5	14	23
• 15	6	24	6	15	24	6	15	24
7	16	25	7	16	25	7	16	25
• 17	8	26	8	17	26	8	17	26
18	9	27	• 18	9	27	9	18	27

Note  $aA_i$  and  $aA_{i+1}$  are near for each  $i = 0, \dots, 4$ , so their images have the same first coordinate. Thus the images of  $aA$  and  $aB$  have the same first coordinate. □

To conclude the proof of Proposition 4.17, we note that for any atoms  $aA$  and  $aB$  having the same first coordinate, that  $B$  can be formed by repeatedly swapping two elements in  $A$  that belong to the same block of  $a$ . So the above claim shows the images of  $aA$  and  $aB$  have the same first coordinate. □

We next consider matters for images of second coordinates of atoms.

**PROPOSITION 4.19.** *Suppose  $a, b$  permute and  $a \cap b = \Delta$ . Let  $C = a \circ b$  and define*

$$\mathcal{Z}(a, b) = \{cC : a, b, c \text{ is a factor triple}\}$$

*Then  $\mathcal{Z}(a, b)$  is those atoms  $cC$  where there are an  $aA \in \mathfrak{X}(a, b)$  and  $bB \in \mathcal{Y}(a, b)$  with  $aA, bB, cC$  pairwise orthogonal. Further, there are  $32 \cdot 32$  elements in  $\mathcal{Z}(a, b)$ .*

*Proof.* Each such orthogonal triple  $a, b, c$  gives atoms  $a(b \circ c)$ ,  $b(a \circ c)$  and  $c(a \circ b)$ . These are pairwise orthogonal atoms with the first and second belonging to  $\mathfrak{X}(a, b)$  and  $\mathcal{Y}(a, b)$  respectively, and the third to  $\mathcal{Z}(a, b)$ . Any two of these atoms determine the third, and our result follows. □

**DEFINITION 4.20.** Call  $\mathfrak{X}$  a slab if it is a set of 36 atoms and there is another set  $\mathcal{Y}$  of 36 atoms with  $\mathfrak{X} \perp \mathcal{Y}$ . Call  $\mathfrak{X}, \mathcal{Y}, \mathcal{Z}$  a triple if  $\mathfrak{X} \perp \mathcal{Y}$  and the members of  $\mathcal{Z}$  are exactly the atoms making up blocks with atoms from  $\mathfrak{X}$  and  $\mathcal{Y}$ .

We have seen in Proposition 4.4 that each slab  $\mathfrak{X}$  is of the form  $\mathfrak{X}(a, b)$  for some small  $a, b$ . These  $a, b$  are uniquely determined as  $a$  is the first component of members of  $\mathfrak{X}$  and  $b$  is the intersection of the second components of  $\mathfrak{X}$ . So a slab  $\mathfrak{X}$  determines uniquely its companion  $\mathcal{Y}$  and the resulting set  $\mathcal{Z}$  of atoms making up blocks with elements of  $\mathfrak{X}$  and  $\mathcal{Y}$ . So  $\mathfrak{X}$  determines the triple  $\mathfrak{X}, \mathcal{Y}, \mathcal{Z}$ .

**PROPOSITION 4.21.** *If  $\mathfrak{X}, \mathcal{Y}, \mathcal{Z}$  is a triple, then any two atoms in  $\mathcal{Z}$  have the same second coordinate, and the images of these atoms under an automorphism  $\Phi$  of  $\text{FACT } X$  have the same second coordinate.*

*Proof.* From the comments above, this triple is  $\mathfrak{X}(a, b), \mathcal{Y}(a, b), \mathcal{Z}(a, b)$  for some  $a, b$ . The second coordinate of members of  $\mathcal{Z}$  must then be  $a \circ b$ , so all members of  $\mathcal{Z}$  have the same second coordinate. The images of  $\mathfrak{X}, \mathcal{Y}, \mathcal{Z}$  under  $\Phi$  form a triple. As members of  $\mathfrak{X}$  have the same first coordinate, by Proposition 4.17 their images under  $\Phi$  have the same first coordinate  $a'$ , and the images of members of  $\mathcal{Y}$  have the same first coordinate  $b'$ . So the image of  $\mathfrak{X}$  is  $\mathfrak{X}(a', b')$ , the image of  $\mathcal{Y}$  is  $\mathcal{Y}(a', b')$ , hence the image of  $\mathcal{Z}$  is  $\mathcal{Z}(a', b')$ . Therefore the images of members of  $\mathcal{Z}$  all have the same second coordinate  $a' \circ b'$ .  $\square$

Earlier, we defined nearness for atoms with the same first coordinate. We now define a notion of nearness for atoms with the same second coordinate. Here we use  $\oplus$  for the symmetric difference of sets.

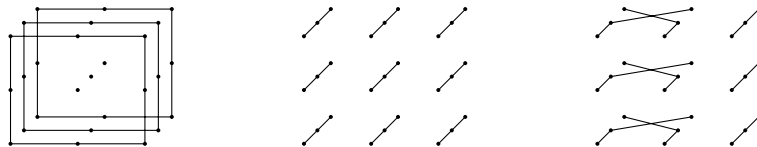
**DEFINITION 4.22.** Atoms  $aA$  and  $bA$  with the same second coordinate are near if  $b$  is formed from  $a$  as follows. Find by 6 elements  $x_1, \dots, x_6$  in a block  $A_1$  of  $A$  and let  $a_1, \dots, a_6$  be blocks of  $a$  with  $x_i \in a_i$ . Let  $b$  have blocks  $b_1, \dots, b_9$  such that for  $i = 1, 3, 5$   $b_i = a_i \oplus \{a_1, a_{i+1}\}$  and  $b_{i+1} = a_{i+1} \oplus \{a_i, a_{i+1}\}$ , and  $b_i = a_i$  for  $i = 7, 8, 9$ .

So  $aA$  and  $bA$  are near if  $b$  is formed from  $a$  by making three non-overlapping swaps of elements all in one block of  $A$ . A typical example is shown below where we use like symbols at left to indicate the the rows of the pairs of swaps.

$\triangle$	1	10	19	1	10	20
$\triangle$	2	11	20	2	11	19
*	3	12	21	3	12	22
*	4	13	22	4	13	21
•	5	14	23	5	14	24
•	6	15	24	6	15	23
	7	16	25	7	16	25
	8	17	26	8	17	26
	9	18	27	9	18	27

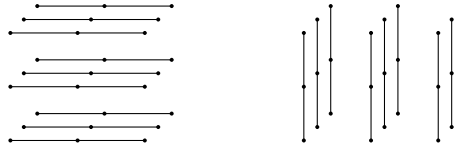
**LEMMA 4.23.** *If  $aA$  and  $bA$  are near, there is a triple  $\mathfrak{X}, \mathcal{Y}, \mathcal{Z}$  with  $aA, bA \in \mathcal{Z}$ .*

*Proof.* Reverting to our earlier method of representing  $X$ , assume elements of  $X$  are triples such as 012 arranged on the  $x, y, z$ -axes. We assume without loss of generality that  $A, a$ , and  $b$  are as follows. The blocks of  $A$  are the planes  $x = 0, 1, 2$  and  $A$  is at left below; the blocks of  $a$  are lines parallel to the  $x$ -axis shown in the middle below; and the small relation  $b$  is shown at right below. Any near  $aA$  and  $bA$  can be realized in this way for some enumeration of  $X$ .



Then consider the small relation  $p$  whose blocks are lines parallel to the  $y$ -axis, and the small relation  $q$  whose blocks are lines parallel to the  $z$ -axis. We have shown  $p, q$  below.

Clearly  $a, p, q$  are an orthogonal triple. To see  $b, p, q$  are an orthogonal triple, it is enough to see  $b, p, q$  pairwise permute, and  $b \cap (p \circ q) = p \cap (b \circ q) = q \cap (b \circ p) = \Delta$ . Thus  $aA$  and  $bA$  belong to  $\mathcal{Z}(p, q)$ .  $\square$



**PROPOSITION 4.24.** *If  $aA$  and  $bA$  are atoms with the same second coordinate, then their images under an automorphism  $\Phi$  of FACT  $X$  have the same second coordinate.*

*Proof.* We first show that if  $aA$  and  $cA$  are such that  $a$  and  $c$  agree except for having two elements in the same block of  $A$  interchanged, then  $\Phi(aA)$  and  $\Phi(cA)$  have the same second coordinate. Consider the situation below that represents four atoms  $aA, uA, vA, cA$  where  $aA$  and  $cA$  are such that  $a, c$  agree except for two elements swapped. Each pair of elements in this sequence are near atoms with the same second coordinate, so by Lemma 4.23 and Proposition 4.21 their images have the same second coordinate. Thus  $\Phi(aA)$  and  $\Phi(cA)$  have the same second coordinate. Up to rearrangement of elements of  $X$ , this argument is general.

1	10	19	1	10	19	$\Delta$ 1	10	19	1	10	20
$\Delta$ 2	11	20	$\Delta$ 2	11	21	$\Delta$ 2	11	20	2	11	19
$\Delta$ 3	12	21	$\Delta$ 3	12	20	3	12	21	3	12	21
4	13	22	$\star$ 4	13	22	$\star$ 4	13	23	4	13	22
5	14	23	$\star$ 5	14	23	$\star$ 5	14	22	5	14	23
$\star$ 6	15	24	$\bullet$ 6	15	25	6	15	24	6	15	24
$\star$ 7	16	25	$\bullet$ 7	16	24	7	16	25	7	16	25
$\bullet$ 8	17	26	8	17	27	$\bullet$ 8	17	27	8	17	26
$\bullet$ 9	18	27	9	18	26	$\bullet$ 9	18	26	9	18	27

To complete the proof we have only to note that for any  $aA$  and  $bA$  with the same second coordinate, we can transform  $a$  into  $b$  through a series of moves, each swapping two elements belonging to the same block of  $A$ . □

Propositions 4.17 and 4.24 allow the following definition.

**DEFINITION 4.25.** For an automorphism  $\Phi$  of FACT  $X$ , define endomorphisms  $\Phi_S$  of the small relations and  $\Phi_L$  of the large relations as follows.

$$\begin{aligned} \Phi_S a &= \text{the first coordinate of any } \Phi(aA) \text{ where } aA \text{ is an atom} \\ \Phi_L A &= \text{the second coordinate of any } \Phi(aA) \text{ where } aA \text{ is an atom} \end{aligned}$$

The following is easily verified from the definition.

**LEMMA 4.26.** *For  $\Phi, \Psi$  automorphisms of FACT  $X$  we have*

- (1)  $(\Psi \circ \Phi)_S = \Phi_S \circ \Psi_S$
- (2)  $(\Psi \circ \Phi)_L = \Phi_L \circ \Psi_L$

*Further, if  $\Phi$  is the identity map on FACT  $X$ , both  $\Phi_S$  and  $\Phi_L$  are identity maps.*

It follows that  $\Phi_S$  is a permutation of the set of small relations of  $X$ ,  $\Phi_L$  is a permutation of the large relations, and that the obvious maps  $S$  and  $L$  from the automorphism group of FACT  $X$  to the permutation groups of the small and large relations are group homomorphisms.

**THEOREM 4.27.** *There is a group embedding  $R$  of the automorphism group of FACT  $X$  into the group of order-automorphisms of the poset  $\text{REQ } X$  taking  $\Phi$  to  $\Phi_R$  where*

$$\Phi_R x = \begin{cases} \Phi_S x & \text{if } x \text{ is small} \\ \Phi_L x & \text{if } x \text{ is large} \end{cases}$$



*Proof.* From Lemma 4.26 it follows that each  $\Phi_R$  is a permutation of the regular equivalence relations, and that  $R$  is a group homomorphism from the automorphism group of  $\text{FACT } X$  to the group of permutations of  $\text{REQ } X$ . From the definition, it is trivial that  $\Phi_R$  is the identity iff  $\Phi$  is the identity, so  $R$  is a group embedding. It remains only to show that each  $\Phi_R$  is an order-embedding. For this, we know  $R$  is a group homomorphism, so it is enough to show  $\Phi_R$  is order-preserving.

Suppose  $a$  is small and  $A$  is large with  $a \leq A$ . Then there is a small  $b$  with  $a \cap b = \Delta$ ,  $a$  permuting with  $b$ , and  $a \circ b = A$ . So there is a triple  $\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$  with the first coordinate of members of  $\mathfrak{X}$  being  $a$ , the first coordinate of members of  $\mathfrak{Y}$  being  $b$ , and the second coordinate of members of  $\mathfrak{Z}$  being  $A$ . As we have seen, the images of  $\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$  under  $\Phi$  are a triple with the first coordinate of members of the image of  $\mathfrak{X}$  being  $\Phi_S a$ , the first coordinate of members of the image of  $\mathfrak{Y}$  being  $\Phi_S b$ , and the second coordinate of members of the image of  $\mathfrak{Z}$  being  $\Phi_L A$ . This implies  $\Phi_S a \leq \Phi_L A$ , and shows  $\Phi_R$  is order-preserving.  $\square$

## 5. The case of a 27-element set — the second half

Here we complete the proof that for  $X$  a 27-element set, the map  $\Gamma$  gives an isomorphism from the permutation group of  $X$  to the group of automorphisms of  $\text{FACT } X$ . In particular, we show the automorphisms of the poset  $\text{REQ } X$  correspond to permutations of the set  $X$ .

**LEMMA 5.1.** *For small  $a, b$ , if  $\text{TRCL}(a \cup b)$  has 7 blocks of 3 and 1 block of 6, then  $a, b$  have 70 large upper bounds.*

*Proof.* Note that any equivalence relation containing  $a$  joins together blocks of  $a$ , and this includes  $\text{TRCL}(a \cup b)$ . As  $\text{TRCL}(a \cup b)$  has 7 blocks of 3 and 1 block of 6, the large relations containing this transitive closure are formed by picking one of the blocks of 3 to match with the block of 6, and there are 7 ways to do this, then splitting the remaining 6 blocks of 3 into two batches of 3, and there are 10 ways to do this.  $\square$

We extend this notion to other pairs of elements. Here we write  $(1-6, 7-3) = 70$  to mean if  $\text{TRCL}(a \cup b)$  has 1 block of 6, and 7 blocks of 3, then  $a, b$  have 70 large upper bounds in common. We will not prove the following result, but will use it. Its proof is a matter of counting along the lines above.

**LEMMA 5.2.** *For small relations  $a, b$ , we have the following.*

$$\begin{array}{llll} (9-3) = 280 & (1-6, 7-3) = 70 & (1-9, 6-3) = 10 & (2-6, 5-3) = 20 \\ (3-6, 3-3) = 6 & (4-6, 1-3) = 0 & (1-9, 1-6, 4-3) = 4 & (1-9, 2-6, 2-3) = 2 \\ (1-9, 3-6) = 0 & (2-9, 3-3) = 1 & (2-9, 1-6, 1-3) = 1 & (3-9) = 1 \end{array}$$

**DEFINITION 5.3.** Suppose  $a$  is small and  $a_1, \dots, a_9$  are the blocks of  $a$ . Define

$$\mathfrak{X}(a : a_i, a_j) = \{b : b \text{ is small and } n \neq i, j \implies a_n \text{ is a block of } b\}.$$

Our next aim is be able to abstractly recognize such sets of small relations in the poset of regular equivalence relations. This will show such sets are mapped in a well-behaved manner by automorphisms of  $\text{REQ } X$ .

**LEMMA 5.4.**  *$\mathfrak{X}(a : a_i, a_j)$  has 10 elements, and any two distinct elements of this set have 70 large upper bounds in common. Conversely, any set  $\mathfrak{X}$  of 10 small relations where any two have 70 large upper bounds is of the form  $\mathfrak{X}(a : a_i, a_j)$  where  $a$  can be chosen to be any member of  $\mathfrak{X}$  and  $a_i \cup a_j$  is the same no matter the  $a$  chosen.*

*Proof.* The elements of  $\mathfrak{X}(a : a_i, a_j)$  are those small  $b$  that share at least 7 blocks with  $a$ . These are the  $b$ 's formed by taking these 7 blocks of  $a$ , then splitting up  $a_i \cup a_j$  into two groups of 3, where the order of these groups, and in these groups, doesn't matter. So there are 10 such  $b$ , one of which will be  $a$ . Lemma 5.1 shows that any two distinct members of this group have 70 large upper bounds in common.

Conversely, suppose  $\mathfrak{X}$  is such a set. Pick any element in this, say  $a$ . For another element  $b$  in this set to have 70 large upper bounds in common with  $a$ , it must be that  $\text{TRCL}(a \cup b)$  has 1 block of 6 and 7 blocks of 3. So  $a, b$  have 7 blocks in common. Take a third element  $c$  in  $\mathfrak{X}$ . We must have that any two of  $a, b, c$  share 7 blocks. Say  $a, b$  share the blocks  $a_3, \dots, a_9$  of  $a$ . Then as  $a \neq b$  we have neither  $a_1, a_2$  is a block of  $b$ . So the blocks of  $b$  are  $b_1, b_2, a_3, \dots, a_9$  where neither  $b_1, b_2$  equals  $a_1, a_2$ . Suppose  $a, c$  do not share the same 7 blocks  $a_3, \dots, a_9$ . Say  $a_3$  is not a block of  $c$ . Then for  $c$  to share 7 blocks with  $a$  we must have one of  $a_1, a_2$  is a block of  $c$ . Say  $a_1$  is a block of  $c$ . Then neither  $b_1, b_2$  can be a block of  $c$ , since both contain some, but not all of  $a_1$ . Also  $a_3$  is not a block of  $c$ , but is a block of  $b$ . So  $c$  cannot share 7 blocks with  $b$ . Thus all members of  $\mathfrak{X}$  have the same 7 blocks of  $a$  in common. So  $\mathfrak{X} = \mathfrak{X}(a : a_1, a_2)$ . If we had chosen a different element from  $\mathfrak{X}$  to begin, say  $b$ , the blocks  $b_i, b_j$  would have been different, but  $b_i \cup b_j$  would equal  $a_1 \cup a_2$ .  $\square$

**DEFINITION 5.5.** A set  $\mathfrak{X}$  of small relations is called a collapse if it satisfies the conditions of Lemma 5.4. We say  $a, b$  are neighbours and write  $a \sim b$  if they both belong to a collapse.

**DEFINITION 5.6.** Two collapses  $\mathfrak{X}$  and  $\mathfrak{Y}$  are said to share a block if  $\mathfrak{X} \cap \mathfrak{Y} \neq \emptyset$  and no  $a, b$  in  $\mathfrak{X} \cup \mathfrak{Y}$  have exactly 20 common large upper bounds.

**LEMMA 5.7.** *Let  $a$  be a small relation with blocks  $a_1, \dots, a_9$ . Then the collapses  $\mathfrak{X}(a : a_i, a_j)$  and  $\mathfrak{X}(a : a_m, a_n)$  share a block iff one of  $i, j$  equals one of  $m, n$ .*

*Proof.* Suppose these collapses share a block. If  $a_i, a_j, a_m, a_n$  are all different, then there would be elements  $b \in \mathfrak{X}$  and  $c \in \mathfrak{Y}$  with  $\text{TRCL}(b \cup c)$  having 2 blocks of 6 and 5 blocks of 3, hence by Lemma 5.2, the pair  $b, c$  would have 20 upper bounds. So one of  $a_i, a_j$  equals one of  $a_m, a_n$ . Conversely, if  $i = m$ , then for any  $b, c$  in  $\mathfrak{X}(a : a_i, a_j) \cup \mathfrak{X}(a : a_i, a_n)$  we have  $\text{TRCL}(b \cup c)$  has either 1 block of 9 and 6 blocks of 3 (if one is from each set), or has 1 block of 6 and 7 blocks of 3 (if both are from the same). In either case, by Lemma 5.2 they do not have exactly 20 upper bounds.  $\square$

**LEMMA 5.8.** *Each small relation  $a$  is in exactly 36 collapses.*

*Proof.* If  $a$  is in a collapse  $\mathfrak{X}$ , then by Lemma 5.4, we have  $\mathfrak{X} = \mathfrak{X}(a : a_i, a_j)$  for two blocks  $a_i, a_j$  of  $a$ . There are 36 ways to choose these two blocks, since their order does not matter.  $\square$

**DEFINITION 5.9.** A 3-element subset  $\alpha$  of  $X$  is called a small block. For such  $\alpha$ , set

$$\mathfrak{X}_\alpha = \{a : \alpha \text{ is a block of } a\}.$$

**LEMMA 5.10.** *Let  $\mathfrak{X}$  be a set of  $24!/(8!)(3!)^8$  small relations with  $\sim$  the restriction of the neighbour relation to  $\mathfrak{X}$ , and suppose the following hold for all  $a, b, c \in \mathfrak{X}$ .*

- (1) 28 of the collapses containing  $a$  are subsets of  $\mathfrak{X}$ .
- (2) 8 of the collapses containing  $a$  intersect  $\mathfrak{X}$  only in  $\{a\}$ .
- (3) Any two collapses of  $a$  that intersect  $\mathfrak{X}$  only in  $\{a\}$  share a block.
- (4) If  $a \sim b, c$  and  $b, c$  have 20 upper bounds, there is  $d \neq a$  in  $\mathfrak{X}$  with  $b, c \sim d$ .

*Then  $\mathfrak{X} = \mathfrak{X}_\alpha$  for some small block  $\alpha$ . Conversely, each  $\mathfrak{X}_\alpha$  satisfies these properties.*

**Proof.** We first show  $\mathfrak{X}_\alpha$  satisfies these properties. That it has the indicated number of elements is routine. Suppose  $a \in \mathfrak{X}_\alpha$ , and that the blocks of  $a$  are  $a_1, \dots, a_9$  with  $a_1 = \alpha$ . By Lemma 5.4 the collapses containing  $a$  are exactly the  $\mathfrak{X}(a : a_i, a_j)$ . If either  $i, j$  equals 1, then the only element of this collapse having  $\alpha$  as a block is  $a$ , and if  $i, j \neq 1$ , then all elements of this collapse have  $\alpha$  as a block, so this collapse is contained in  $\mathfrak{X}_\alpha$ . So there are 28 collapses containing  $a$  that are contained in  $\mathfrak{X}_\alpha$  and 8 that intersect  $\mathfrak{X}_\alpha$  only in  $\{a\}$ . Any two collapses that intersect  $\mathfrak{X}_\alpha$  only in  $\{a\}$  are of the form  $\mathfrak{X}(a : a_1, a_i)$  and  $\mathfrak{X}(a : a_1, a_j)$ , so by Lemma 5.7 they share a block. For the final condition, suppose  $b, c \in \mathfrak{X}_\alpha$  with  $a \sim b, c$  and that  $b, c$  have 20 large upper bounds. This means  $b$  is in a collapse of  $a$ , and this collapse must be of the form  $\mathfrak{X}(a : a_i, a_j)$  with  $i, j \neq 1$ , and similarly  $c$  is in  $\mathfrak{X}(a : a_m, a_n)$  with  $m, n \neq 1$ . Since  $b, c$  have 20 large upper bounds,  $\text{TRCL}(b \cup c)$  has 2 blocks of 6 and 5 blocks of 3, and the two blocks of 6 are  $a_i \cup a_j$  and  $a_m \cup a_n$ . So  $i, j, m, n$  are all distinct. Form  $d$  to behave like  $b$  on  $a_i \cup a_j$  and like  $c$  on  $a_m \cup a_n$ , and to agree with  $a$  elsewhere. Then  $d$  is in the collapse  $\mathfrak{X}(b : a_m, a_n)$  and also in the collapse  $\mathfrak{X}(c : a_i, a_j)$ , so  $b, c \sim d$ . As  $i, j, m, n \neq 1$ , we have  $d \in \mathfrak{X}$ . So  $\mathfrak{X}_\alpha$  satisfies these conditions.

For the forward direction, suppose that  $\mathfrak{X}$  is a set with the indicated number of small relations that satisfies these conditions.

**CLAIM 5.11.** *For  $a \in \mathfrak{X}$  with blocks  $a_1, \dots, a_9$ , there is a block  $a_k$ , that we denote  $\alpha(a)$ , with  $\mathfrak{X}(a : a_i, a_j) \subseteq \mathfrak{X}$  if  $i, j \neq k$  and  $\mathfrak{X}(a : a_i, a_j) \cap \mathfrak{X} = \{a\}$  if either  $i, j = k$ .*

**Proof.** There are 8 collapses  $\mathfrak{X}(a : a_i, a_j)$  that intersect  $\mathfrak{X}$  only in  $\{a\}$ , and any two of these share a block. So they must share the same block, some  $a_k$ , and these must be all collapses of  $a$  using this block.  $\square$

**CLAIM 5.12.** *If  $a, b \in \mathfrak{X}$  and  $a \sim b$ , then  $\alpha(a) = \alpha(b)$ .*

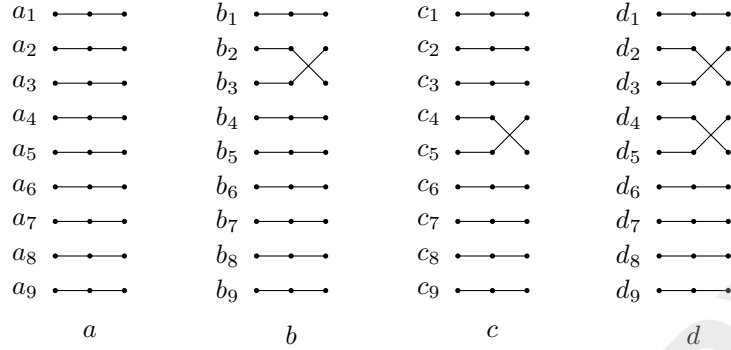
**Proof.** Suppose  $a$  has blocks  $a_1, \dots, a_9$  and  $\alpha(a) = a_1$ . As  $b \in \mathfrak{X}$  and  $a \sim b$  we have  $b \in \mathfrak{X}(a : a_i, a_j)$  for some  $i, j \neq 1$ . We assume  $b \in \mathfrak{X}(a : a_2, a_3)$ . Let the blocks of  $b$  be  $b_1, \dots, b_9$  with the numbering chosen so that  $b_1 = a_1$ ,  $b_2 \cup b_3 = a_2 \cup a_3$  and  $b_i = a_i$  for  $i = 4, \dots, 9$ . We must show  $\alpha(b) = b_1$ .

We know  $\alpha(b) \neq b_2, b_3$  since  $a \in \mathfrak{X}(b : b_2, b_3)$  showing that this collapse does not intersect  $\mathfrak{X}$  only in  $\{b\}$ . We show  $\alpha(b) \neq b_4, \dots, b_9$ , hence  $\alpha(b) = b_1$  as required. We provide the argument to show  $\alpha(b) \neq b_4$ , the others follow by symmetry.

Choose any element  $c$  in  $\mathfrak{X}(a : a_4, a_5)$  distinct from  $a$ . Let the blocks of  $c$  be numbered  $c_1, \dots, c_9$  with  $c_i = a_i$  for  $i \neq 4, 5$  and with  $c_4 \cup c_5 = a_4 \cup a_5$ . Then  $\text{TRCL}(b \cup c)$  has 2 blocks of 6, namely  $a_2 \cup a_3$  and  $a_4 \cup a_5$ , and 5 blocks of 3, the blocks  $a_1, a_6, \dots, a_9$ . So  $b, c$  have 20 large upper bounds. Then by condition (4) there is  $d \in \mathfrak{X}$  distinct from  $a$  with  $b, c \sim d$ . Since  $d$  is in a collapse of  $b$  and a collapse of  $c$  and differs from  $a$ , the only possibility for  $d$  is to have  $d$  agree with  $a$  (and with  $b, c$ ) on  $a_1, a_6, \dots, a_9$  and for  $d$  to be such that  $d$  agrees with  $b$  on  $a_2 \cup a_3$  and with  $c$  on  $a_4 \cup a_5$ . As  $b \sim d$  we must have  $d \in \mathfrak{X}(b : b_i, b_j)$ , and clearly  $i, j$  must be 4, 5. This shows  $\mathfrak{X}(b : b_4, b_5)$  does not intersect  $\mathfrak{X}$  only in  $b$ , hence  $\alpha(b) \neq b_4$ .  $\square$

**CLAIM 5.13.** *If  $a \in \mathfrak{X}$ , then  $\mathfrak{X}_{\alpha(a)} \subseteq \mathfrak{X}$ .*

**Proof.** Choose  $a \in \mathfrak{X}$ . Note that if  $b$  is obtained from  $a$  by swapping two elements in blocks of  $a$  other than  $\alpha(a)$ , then  $b \in \mathfrak{X}$  and  $a \sim b$ , so by Claim 5.12,  $\alpha(a) = \alpha(b)$ . So if  $b^0, b^1, \dots, b^n$  is a sequence of relations with  $b^0 = a$  and each obtained from the previous by switching two elements not contained in the block  $\alpha(a)$ , then  $\alpha(b^i) = \alpha(a)$  and  $b^i \in \mathfrak{X}$  for each  $i \leq n$ . We claim that any  $c$  having  $\alpha(a)$  as a block can be obtained as  $b^n$  for some such sequence  $b^0, \dots, b^n$  beginning with  $b^0 = a$ . Suppose not. Then among all elements  $b^n$  obtained by such a sequence, choose one, say  $b$ , that agrees with  $c$  on as many blocks as possible. Suppose the blocks of  $b$  are  $b_1, \dots, b_9$ , the



blocks of  $c$  are  $c_1, \dots, c_9$ , that  $b, c$  agree on blocks  $b_1, \dots, b_k$  and that  $b_1 = c_1 = \alpha(a)$ . We may also assume that block  $b_{k+1}$  is the block of  $b$  having the most elements in common with  $c_{k+1}$ . Note  $b_{k+1}$  and  $c_{k+1}$  have either one or two elements in common, and the other elements in  $c_{k+1}$  are in blocks  $b_{k+1}, \dots, b_9$  since  $b_i = c_i$  for  $i \leq k$ . If  $b_{k+1}$  and  $c_{k+1}$  agree on two elements, we may assume the third element of  $c_{k+1}$  in the block  $b_{k+2}$ . Then by an appropriate swapping of elements in the blocks  $b_{k+1}, b_{k+2}$  of  $b$ , we can form another term  $b^{n+1}$  to put at the end of our sequence that agrees with  $c$  on  $k + 1$  blocks. If  $b_{k+1}$  contains only one element of  $c_{k+1}$ , then we may assume the other two elements of  $c_{k+1}$  are in  $b_{k+2}, b_{k+3}$ . We can then extend our sequence by forming  $b^{n+1}, b^{n+2}$  first by swapping two elements in  $b_{k+1}, b_{k+2}$ , then performing one more swap to put the element from  $b_{k+3}$  into the block to form  $c_{k+1}$ .  $\square$

As  $\mathfrak{X}_{\alpha(a)} \subseteq \mathfrak{X}$  and both have  $24!/(8!)(3!)^8$  elements, they are equal.  $\square$

This result will allow us to transfer an automorphism of the poset of regular equivalence relations to a certain kind of permutation of the set of small blocks. The key point is that for an automorphism  $\Lambda$  of  $\text{REQ } X$ , Lemma 5.10 shows that for a small block  $\alpha$ , the image  $\Lambda[\mathfrak{X}_\alpha]$  is a set  $\mathfrak{X}_\beta$  for some small block  $\beta$ .

**DEFINITION 5.14.** Let  $\text{BLOCK } X = \{\alpha : \alpha \text{ is a small block of } X\}$ . We then define a permutation  $\rho$  of this set to be special if for all small blocks  $\alpha, \beta, \gamma$

- (1)  $|\alpha \cap \beta| = |\rho(\alpha) \cap \rho(\beta)|$ .
- (2)  $\gamma \subseteq \alpha \cup \beta$  iff  $\rho(\gamma) \subseteq \rho(\alpha) \cup \rho(\beta)$ .

One easily sees that the special permutations of  $\text{BLOCK } X$  form a subgroup of its permutation group.

**PROPOSITION 5.15.** *There is an embedding  $B$  of the automorphism group of  $\text{REQ } X$  into the group of special permutations of  $\text{BLOCK } X$  taking  $\Lambda$  to  $\Lambda_B$  where*

$$\Lambda_B(\alpha) = \beta \quad \text{iff} \quad \Lambda[\mathfrak{X}_\alpha] = \mathfrak{X}_\beta.$$

*Proof.* Suppose  $\alpha$  is a small block and  $\Lambda$  is an automorphism of  $\text{REQ } X$ . The set  $\mathfrak{X}_\alpha$  satisfies the four conditions in Lemma 5.10. These conditions involve the notion of a collapse, the numbers of collapses containing an element of  $\mathfrak{X}_\alpha$  that are contained in  $\mathfrak{X}_\alpha$  or nearly disjoint from this set, whether certain collapses share a block, and a statement involving numbers of upper bounds. Lemma 5.4 shows the image of a collapse under an automorphism is a collapse, and the definition of two collapses sharing a block is clearly preserved under automorphisms. Thus the image  $\Lambda[\mathfrak{X}_\alpha]$  satisfies the conditions of Lemma 5.10, hence is  $\mathfrak{X}_\beta$  for some small block  $\beta$ . The definition of  $\mathfrak{X}_\beta$  shows the choice of  $\beta$  is unique.

These comments show that for each automorphism  $\Lambda$  of REQ  $X$ , there is a map  $\Lambda_B$  from BLOCK  $X$  to itself, temporarily called an endomorphism of this unstructured set, defined by  $\Lambda_B(\alpha) = \beta$  iff  $\Lambda[\mathfrak{X}_\alpha] = \mathfrak{X}_\beta$ . So there is a map  $B$  from the automorphism group of REQ  $X$  to the endomorphism monoid of the set of small blocks. Clearly  $B$  preserves composition and the identity map, so  $B$  is a homomorphism from the automorphism group of REQ  $X$  to the permutation group of the small blocks. To see  $B$  is one-one, suppose  $\Lambda \neq \text{id}$ . Then  $\Lambda(a) \neq a$  for some small relation  $a$ , so there is a block  $\alpha$  of  $a$  that is not a block of  $\Lambda(a)$ . It follows that  $\Lambda[\mathfrak{X}_\alpha] \neq \mathfrak{X}_\alpha$ . So  $B(\Lambda) \neq \text{id}$ . Thus  $B$  is an embedding. It remains to show each  $\Lambda_B$  is a special permutation.

**CLAIM 5.16.**  $|\alpha \cap \beta| = |\Lambda_B(\alpha) \cap \Lambda_B(\beta)|$ .

**PROOF.** Note  $\alpha$  and  $\beta$  are disjoint iff  $\mathfrak{X}_\alpha$  and  $\mathfrak{X}_\beta$  are not disjoint. It follows that  $|\alpha \cap \beta| = 0$  iff  $|\Lambda_B(\alpha) \cap \Lambda_B(\beta)| = 0$ . As  $\Lambda_B$  is a permutation, we have  $\alpha = \beta$  iff  $\Lambda_B(\alpha) = \Lambda_B(\beta)$  and the case of an intersection in 3 elements follows. Once we know that  $\alpha$  and  $\beta$  intersect in either 1 or 2 elements, we can distinguish the cases as follows:  $\alpha$  and  $\beta$  intersect in 2 elements iff for any small  $a$  having  $\alpha$  as a block, there is a small  $b$  having  $\beta$  as a block, so that  $\text{TRCL}(a \cup b)$  has 1 block of 6 and 7 blocks of 3. By Lemma 5.2 this condition on  $\text{TRCL}(a \cup b)$  occurs iff  $a, b$  have 70 large upper bounds. So it follows that  $|\alpha \cap \beta| = 2$  iff  $|\Lambda_B(\alpha) \cap \Lambda_B(\beta)| = 2$ . The statement for an intersection in one element follows by elimination.  $\square$

**CLAIM 5.17.**  $\gamma \subseteq \alpha \cup \beta$  iff  $\Lambda_B(\gamma) \subseteq \Lambda_B(\alpha) \cup \Lambda_B(\beta)$ .

**PROOF.** We show  $\gamma \subseteq \alpha \cup \beta$  implies  $\Lambda_B(\gamma) \subseteq \Lambda_B(\alpha) \cup \Lambda_B(\beta)$ . The other direction follows by the same result for the inverse  $\Lambda^{-1}$ . We argue the contrapositive. Suppose  $x \in \Lambda_B(\gamma)$  and  $x$  is not in  $\Lambda_B(\alpha) \cup \Lambda_B(\beta)$ . Choose two other elements  $y, z$  not belonging to  $\Lambda_B(\alpha) \cup \Lambda_B(\beta)$ , and let  $\delta$  be the small block with  $\Lambda_B(\delta) = \{x, y, z\}$ . Then  $\Lambda_B(\delta)$  is disjoint from both  $\Lambda_B(\alpha)$  and  $\Lambda_B(\beta)$ , so  $\delta$  is disjoint from  $\alpha$  and  $\beta$ . But  $\Lambda_B(\delta)$  intersects  $\Lambda_B(\gamma)$  non-trivially, so  $\gamma$  contains an element of  $\delta$ , hence  $\gamma$  is not contained in  $\alpha \cup \beta$ .  $\square$

This concludes the proof of the proposition.  $\square$

We turn to our final step, associating to a special permutation  $\rho$  of BLOCK  $X$  a permutation of  $X$ . The key is the following lemma.

**LEMMA 5.18.** *Let  $\rho$  be a special permutation of BLOCK  $X$ . If  $\alpha, \beta, \gamma$  are small blocks with  $\alpha \cap \beta = \{p\}$  and  $\rho(\alpha) \cap \rho(\beta) = \{x\}$ , then  $p \in \gamma \implies x \in \rho(\gamma)$ .*

**PROOF.** Using symmetry, there are four cases.

- (1)  $\gamma$  intersects both  $\alpha$  and  $\beta$  in two elements.
- (2)  $\gamma$  intersects one of  $\alpha, \beta$  in two elements, and the other in one element.
- (3)  $\gamma$  intersects both  $\alpha, \beta$  in one element.
- (4)  $\gamma$  is equal to one of  $\alpha, \beta$ .

We begin with a claim that establishes case (1) and that will be used repeatedly to establish the other cases.

**CLAIM 5.19.** *For any small blocks  $\alpha, \beta, \gamma$ , if  $\gamma$  intersects both  $\alpha, \beta$  in two elements and  $\rho(\alpha) = \{x, y_1, y_2\}$ ,  $\rho(\beta) = \{x, z_1, z_2\}$ , then  $\rho(\gamma)$  is  $\{x, y_i, z_j\}$  for some  $i, j \in \{1, 2\}$ .*

**PROOF.** This is obvious from the fact that special permutations preserve the cardinality of intersections and the pigeonhole principle.  $\square$

**CLAIM 5.20.** *Suppose  $p, q_1, q_2, r_1, r_2$  are distinct elements of  $X$ . There there are unique elements  $x, y_1, y_2, z_1, z_2$  with*

- |   |  |
|---|--|
| (1) $\rho\{p, q_1, q_2\} = \{x, y_1, y_2\}$     | (2) $\rho\{p, r_1, r_2\} = \{x, z_1, z_2\}$      |
| (3) $\rho\{p, q_1, r_1\} = \{x, y_1, z_1\}$     | (4) $\rho\{p, q_2, r_2\} = \{x, y_2, z_2\}$      |
| (5) $\rho\{p, q_1, r_2\} = \{x, y_1, z_2\}$     | (6) $\rho\{p, q_2, r_1\} = \{x, y_2, z_1\}$      |
| (7) $\rho\{q_1, q_2, r_1\} = \{y_1, y_2, z_1\}$ | (8) $\rho\{q_1, q_2, r_2\} = \{y_1, y_2, z_2\}$  |
| (9) $\rho\{q_1, r_1, r_2\} = \{y_1, z_1, z_2\}$ | (10) $\rho\{q_2, r_1, r_2\} = \{y_2, z_1, z_2\}$ |

*Proof.* We have  $\rho\{p, q_1, q_2\}$  and  $\rho\{p, r_1, r_2\}$  intersect in an element. So items (1) and (2) are clear. For item (3) we have  $\{p, q_1, r_1\}$  intersects both of  $\{p, q_1, q_2\}$  and  $\{p, r_1, r_2\}$  in two elements, so by Claim 5.19 we have  $\rho\{p, q_1, r_1\}$  equals  $\{x, y_i, z_j\}$  for some choice of  $i, j$ . At this point we are free to choose the numbering of  $y_1, y_2$  and  $z_1, z_2$  as we please, and we number them to make (3) hold. We again use Claim 5.19 to obtain  $\rho\{p, q_2, r_2\}$  is of the form  $\{x, y_i, z_j\}$  for some  $i, j$ , and as  $\rho\{p, q_1, r_1\}$  and  $\rho\{p, q_2, r_2\}$  must intersect only in one element, it must be as indicated in (4). For (5), the argument for (3) and (4) shows  $\rho\{p, q_1, r_2\} = \{x, y_i, z_j\}$  for some choice of  $i, j$ , and it cannot be either of the results in (3) or (4). As  $\{p, q_1, r_2\}$  is contained in  $\{p, r_1, r_2\} \cup \{p, q_1, r_1\}$ , by the definition of special in Definition 5.14 we have that  $\rho\{p, q_1, r_2\} \subseteq \{x, y_1, z_1, z_2\}$ . So  $\rho\{p, q_1, r_2\} = \{x, y_1, z_2\}$ . For (6),  $\rho\{p, q_2, r_1\}$  is again of the form  $\{x, y_i, z_j\}$  and this is the only choice remaining. For (7), the definition of special shows  $\rho\{q_1, q_2, r_1\} \subseteq \rho\{p, q_1, q_2\} \cup \rho\{p, q_1, r_1\}$ , therefore is a 3-element subset of  $\{x, y_1, y_2, z_1\}$ . The only 3-element subset of this set not already in our list is  $\{y_1, y_2, z_1\}$ . The arguments for (8) through (10) are similar.  $\square$

We now return to the proof of Lemma 5.18. Assume that  $\alpha \cap \beta = \{p\}$ , and  $\rho(\alpha) \cap \rho(\beta) = \{x\}$ , and that  $\gamma$  is a small block with  $p \in \gamma$ . We must show  $x \in \rho(\gamma)$ . Suppose  $\alpha = \{p, q_1, q_2\}$  and  $\beta = \{p, r_1, r_2\}$  and  $x, y_1, y_2, z_1, z_2$  are as in Claim 5.20. We remarked that up to symmetry there were four cases, and proved in Claim 5.19 case (1) where  $\gamma$  intersected both  $\alpha, \beta$  in two elements. Consider the other cases.

Case (2) has  $\gamma$  intersect  $\alpha$  in two elements, and  $\gamma$  intersect  $\beta$  in one element. We may assume  $\gamma = \{p, q_1, s\}$  for some  $s$  not among  $p, q_1, q_2, r_1, r_2$ . Then  $\rho(\gamma)$  intersects  $\rho\{p, q_1, q_2\} = \{x, y_1, y_2\}$  in 2 elements, and is disjoint from  $\rho\{q_2, r_1, r_2\} = \{y_2, z_1, z_2\}$ . So  $x$  belongs to  $\rho(\gamma)$ . Case (3) has  $\gamma$  intersect each of  $\alpha, \beta$  in one element. Assume  $\gamma = \{p, s, t\}$  for some elements  $s, t$  not among  $p, q_1, q_2, r_1, r_2$ . Then  $\rho(\gamma)$  intersects  $\rho\{p, q_1, q_2\} = \{x, y_1, y_2\}$  in 1 element, and is disjoint from  $\rho\{q_1, q_2, r_1\} = \{y_1, y_2, z_1\}$ . So again,  $x$  belongs to  $\rho(\gamma)$ . The final case (4), where  $\gamma$  equals one of  $\alpha, \beta$  is trivial.  $\square$

**PROPOSITION 5.21.** *There is a one-one group homomorphism  $P$  from the group of special permutations of BLOCK  $X$  to the permutation group of  $X$  such that*

$$\alpha \cap \beta = \{p\} \text{ and } \rho(\alpha) \cap \rho(\beta) = \{x\} \implies (P\rho)(p) = x.$$

*Proof.* Suppose  $\rho$  is a special permutation. For any  $p \in X$  we can find small blocks  $\alpha, \beta$  with  $\alpha \cap \beta = \{p\}$ , and as  $\rho$  is special,  $\rho(\alpha) \cap \rho(\beta)$  is a singleton  $\{x\}$ . Suppose  $\alpha'$  and  $\beta'$  are other small blocks with  $\alpha' \cap \beta' = \{p\}$ . Then as  $\rho$  is special,  $\rho(\alpha') \cap \rho(\beta')$  is a singleton. But  $p \in \alpha'$  and  $p \in \beta'$ , and Lemma 5.18 shows  $x \in \rho(\alpha')$  and  $x \in \rho(\beta')$ . So  $\rho(\alpha') \cap \rho(\beta') = \{x\}$ . Thus, we can define a map  $P\rho$  by setting  $(P\rho)(p) = x$  if there are small  $\alpha, \beta$  with  $\alpha \cap \beta = \{p\}$  and  $\rho(\alpha) \cap \rho(\beta) = \{x\}$ .

One sees that  $P$  preserves composition and the identity map, so is a group homomorphism from the special permutations of BLOCK  $X$  to the permutation group of  $X$ . To see it is one-one, suppose  $\rho$  is a special permutation that is not the identity. There there is a small block  $\alpha$  with  $\rho(\alpha) \neq \alpha$ , hence some  $p \in \alpha$  with  $p \notin \rho(\alpha)$ . Find  $\beta$  with  $\alpha \cap \beta = \{p\}$ . Then  $\rho(\alpha) \cap \rho(\beta) \neq \{p\}$ , so  $(P\rho)(p) \neq p$ . Thus  $P\rho \neq \text{id}$ .  $\square$

We recall our many steps. Theorem 1.6 states that  $\Gamma$  is a homomorphism from the permutation group of  $X$  to the automorphism group of the OMP  $\text{FACT } X$ , and Proposition 3.2 shows that  $\Gamma$  is an embedding. Theorem 4.27 shows that  $R$  is a group embedding of the automorphism group of  $\text{FACT } X$  into the automorphism group of the poset  $\text{REQ } X$  of regular equivalence relations on  $X$ . Proposition 5.15 shows there is an embedding  $B$  of the automorphism group of  $\text{REQ } X$  into the group of special permutations of the set  $\text{BLOCK } X$  of all small blocks of  $X$ . Finally, Proposition 5.21 shows there is a group embedding  $P$  of the group of special permutations of  $\text{BLOCK } X$  into the permutation group of  $X$ .

**THEOREM 5.22.** *Each of the following groups are isomorphic:*

- (1) *The automorphism group of  $\text{FACT } X$ .*
- (2) *The automorphism group of the poset  $\text{REQ } X$ .*
- (3) *The group of special permutations of  $\text{BLOCK } X$ .*
- (4) *The permutation group of  $X$ .*

*Further, the maps  $\Gamma$ ,  $R$ ,  $B$ , and  $P$  are isomorphisms.*

**Proof.** We have shown each of these groups are isomorphic to subgroups of another via the indicated maps, and the groups involved are finite.  $\square$

## 6. Further remarks

In this section, we discuss additional results, and a number of open problems. We begin with the following result of Chevalier [9].

**PROPOSITION 6.1.** *For a vector space  $V$ , each order-automorphism of  $\text{FACT } V$  is an OMP automorphism.*

This result came from Chevalier's proof characterizing automorphisms of  $\text{FACT } V$ . The key step in showing that automorphisms essentially work componentwise, is that two atoms of  $\text{FACT } V$  have distinct coatoms upper bounds iff they have the same first or second coordinate. This property is clearly preserved by any order-automorphism as it does not involve the orthocomplementation. For finite vector spaces, one can show somewhat more.

**PROPOSITION 6.2.** *For a finite vector space  $V$ , there is a unique orthocomplementation on  $\text{FACT } V$  compatible with its order structure.*

We will not give the proof, but remark that the key ingredient is Baer's [2] result that any polarity on a finite projective plane has an absolute point. This finiteness condition is needed as it is easily seen that any orthocomplementation on the subspace lattice  $\text{SUB } V$  gives an orthocomplementation on  $\text{FACT } V$ . So  $\text{FACT } \mathbb{R}^3$  will admit many orthocomplementations [4,6]. We do not know if these auxiliary orthocomplementations are orthomodular.

**PROBLEM 6.3.** *If  $X$  is a set that is not small, are all order-automorphisms of  $\text{FACT } X$  OMP automorphisms? Is  $\text{FACT } X$  uniquely orthocomplemented?*

Recall that a state [22,28] on an OMP  $P$  is a map  $\sigma$  from  $P$  to the real unit interval that maps 0 to 0, 1 to 1, and satisfies  $x \perp y \implies \sigma(x \oplus y) = \sigma(x) + \sigma(y)$ . For any OMP whose blocks are all finite, states correspond to maps from the atoms to the real unit interval such that the values on the atoms of any block sum to 1. Clearly, on any OMP whose blocks all have the same finite number  $n$  of atoms, such as  $\text{FACT } V$  for a finite-dimensional vector space  $V$  or  $\text{FACT } X$  for a finite set  $X$ , there is a state taking value  $1/n$  on each atom.

**PROPOSITION 6.4.** *FACT  $\mathbb{Z}_2^3$  has only the state taking value  $1/3$  on the atoms.*

*Proof.* Recall that this OMP has 28 atoms and 28 blocks. By hand, one can enumerate these atoms as  $x_1, \dots, x_{28}$  and these blocks  $B_1, \dots, B_{28}$ , and set up an incidence matrix  $A$  with the columns representing atoms, the rows the blocks, and entry  $A_{ij}$  being either 0 or 1 depending on whether atom  $x_j$  lies in block  $B_i$ . This matrix  $A$  will have each row consisting of three 1's with the other entries 0's. Then states correspond to solutions of the system of equations  $A\vec{x} = \mathbf{1}$  where  $\mathbf{1}$  is the column matrix of all 1's. Using a computer algebra system, the determinant of this matrix is non-zero. So the system has a unique solution, and this is the state taking constant value  $1/3$ .  $\square$

One can easily produce, or find on the web [26], point-line incidence matrices for other small projective planes over finite fields. Automating the above construction of the atom-block incidence matrix as in the proof of Proposition 6.4 and using a software package to solve the system of equations, one obtains the following result. Matlab worksheets containing the needed input matrices are found next to the link for this paper at [20].

**PROPOSITION 6.5.** *For  $V$  a 3-dimensional vector space over a field with 2, 3, 4, 5, 7 elements, then FACT  $V$  has only the constant state taking values  $1/3$  on the atoms.*

If  $X$  is a set with  $p^3$  elements, for  $p$  prime, then each block of FACT  $X$  is a block of some subalgebra isomorphic to FACT  $\mathbb{Z}_p^3$ . The following is then immediate.

**PROPOSITION 6.6.** *For  $X$  a set with  $2^3, 3^3, 5^3$  or  $7^3$  elements, FACT  $X$  has only the state taking constant value  $1/3$  on the atoms.*

For a vector space  $V$  of dimension 2, or a finite set  $X$  where  $|X|$  has only 2 prime factors, the OMPs FACT  $V$  and FACT  $X$  are of the form  $\text{MO}_n$  for some  $n$ . These are known to have infinitely many states.

**PROBLEM 6.7.** *If  $V$  is a finite-dimensional vector space of dimension at least 3, and if  $X$  is a finite set whose cardinality has at least 3 prime factors, is the state taking constant value on the atoms the only state on FACT  $V$  or FACT  $X$ ?*

We next turn our attention to group-valued measures that play an important role in the theory of unigroups [11] of OMPs.

**DEFINITION 6.8.** A group-valued measure on an OMP  $P$  is a map  $\sigma$  from  $P$  into an abelian group  $G$  that satisfies  $\sigma(0) = 0$  and  $x \perp y \implies \sigma(x \oplus y) = \sigma(x) + \sigma(y)$ .

If each block of an OMP  $P$  has the same finite number of atoms, then for any abelian group  $G$  and element  $a \in G$  there is a group-valued measure on  $P$  taking the value  $a$  on each atom of  $P$ . We call these constant measures. Using techniques from Proposition 6.4 and a linear algebra package to solve equations over finite fields, we obtain the following. A Sage program for this is found next to the link for this paper at [20].

**PROPOSITION 6.9.** *Suppose  $k \in \{2, 3, 4, 5, 7\}$ ,  $p \in \{2, 3, 5, 7\}$ , and consider  $\mathbb{Z}_p$ -valued measures on FACT  $V$  where  $V$  is a 3-dimensional vector space over the  $k$ -element field. If  $p$  does not divide  $k$ , then all such measures are constant, and if  $p$  divides  $k$ , then there are  $pk^8$  such measures.*

When considering group valued measures on FACT  $X$  for a finite set  $X$ , we know the situation for an 8-element set as FACT  $X$  is a horizontal sum of copies of FACT  $\mathbb{Z}_2^3$ , so has a huge number of  $\mathbb{Z}_2$ -valued states. For other cases of finite sets of prime power cardinality, we know no more than the obvious fact that  $\mathbb{Z}_p$ -valued states on FACT  $X$  will be constant when  $p$  does not divide  $|X|$ . The appearance of a power of 8 in the above result is perhaps related to the following question.



**PROBLEM 6.10.** *Determine the unigroup of FACT  $V$  for a finite-dimensional vector space  $V$ , and the unigroup of FACT  $X$  for a finite set  $X$ .*

The main open problem of this paper lies in extending results for the 27-element set to the general case. We know the result does not hold when there are only two prime factors, and that it does not hold for a set with  $2^3$  elements. We have no intuition about the behavior for other *small* cases such as a set with  $2^2 \times 3$ , or  $2 \times 3^2$ , or  $2 \times 3 \times 5$ , or  $2^n$  elements. But we suspect that if  $X$  has at least three prime factors bigger than 2, then the situation is well-behaved. We record this below.

**PROBLEM 6.11.** *If  $X$  is a set of sufficiently large size, is the embedding  $\Gamma$  of the permutation group of  $X$  into the automorphism group of FACT  $X$  an isomorphism?*

REFERENCES

- [1] ABRAMSKY, S.—COECKE, B.: *A categorical semantics of quantum protocols*. In: Proceedings of the 19<sup>th</sup> Annual IEEE Symposium on Logic in Computer Science (LICS '04), IEEE Comp. Soc., New York, 2004, pp. 415–425.
- [2] BAER, R.: *Polarities in finite projective planes*, Bull. Amer. Math. Soc. **52** (1946), 77–93.
- [3] BAER, R.: *Linear Algebra and Projective Geometry*, Pure Appl. Math. (Amst.) 2, Elsevier/Academic Press, Amsterdam, 1952.
- [4] BIRKHOFF, G.: *Ordered sets in geometry*. In: Ordered Sets (I. Rival, ed.), Reidel, Dordrecht, 1982, pp. 407–443.
- [5] BURRIS, S.—SANKAPPANAVAR, H. P.: *A Course in Universal Algebra*, Springer, Berlin-Heidelberg-New York, 1981.
- [6] CHEVALIER, G.: *Different orthocomplementations on the subspace lattice of a finite-dimensional complex vector space*, Internat. J. Theoret. Phys. **39** (2000), 565–570.
- [7] CHEVALIER, G.: *Automorphisms of an orthomodular poset of projections*, Internat. J. Theoret. Phys. **44** (2005), 985–998.
- [8] CHEVALIER, G.: *The orthomodular poset of projections of a symmetric lattice*, Internat. J. Theoret. Phys. **44** (2005), 2073–2089.
- [9] CHEVALIER, G.: *Wigner type theorems for projections*, Internat. J. Theoret. Phys. **47** (2008), 69–80.
- [10] DVUREČENSKIJ, A.: *Gleason's Theorem and its Applications*, Kluwer, Dordrecht-Boston-London, 1993.
- [11] FOULIS, D. J.—GREECHIE, R. J.—BENNETT, M. K.: *The transition to unigroups*, Internat. J. Theoret. Phys. **37** (1998), 45–63.
- [12] HARDING, J.: *Decompositions in quantum logic*, Trans. Amer. Math. Soc. **348** (1996), 1839–1862.
- [13] HARDING, J.: *Regularity in quantum logic*, Internat. J. Theoret. Phys. **37** (1998), 1173–1212.
- [14] HARDING, J.: *Axioms of an experimental system*, Internat. J. Theoret. Phys. **38** (1999), 1643–1675.
- [15] HARDING, J.: *States on orthomodular posets of decompositions*, Internat. J. Theoret. Phys. **40** (2001), 1061–1069.
- [16] HARDING, J.: *Orthomodularity of decompositions in a categorical setting*, Internat. J. Theoret. Phys. **45** (2006), 1117–1127.
- [17] HARDING, J.: *The source of the orthomodular law*. In: Handbook of Quantum Logic and Quantum Structures: Quantum Structures (K. Engesser, D. Gabbay, D. Lehman, eds.), Elsevier, Amsterdam, 2007, pp. 555–586.
- [18] HARDING, J.: *A link between quantum logic and categorical quantum mechanics*, Internat. J. Theoret. Phys. **48** (2009), 769–802.
- [19] HARDING, J.: *Daggers, kernels, Baer  $\ast$ -semigroups, and orthomodularity*, J. Philos. Logic **42** (2013), 535–549.
- [20] HARDING, J.—HANNAN, T.: Personal webpage: [www.math.nmsu.edu/jharding](http://www.math.nmsu.edu/jharding).
- [21] HEUNEN, C.—JACOBS, B.: *Quantum logic in dagger kernel categories*, Order **27** (2010), 177–212.
- [22] KALMBACH, G.: *Orthomodular Lattices*, Academic Press, London, 1983.
- [23] KATRNOŠKA, F.: *Logics of idempotents of rings*. In: Proc. Second Winter School on Measure Theory, Lip-tovský Ján, 1990, Jednota Slov. Mat. Fyz., Bratislava, 1990, pp. 100–104.
- [24] MCKENZIE, R.—MCNULTY, G.—TAYLOR, W.: *Algebras, Lattices, Varieties Volume I*, Wadsworth & Brooks/Cole, Monterey, CA, 1987.
- [25] MACKEY, G.: *The Mathematical Foundations of Quantum Mechanics*, W. A. Benjamin, Inc., New York-Amsterdam, 1963.

- [26] MOOREHOUSE, E.: Personal webpage: <http://www.uwo.edu/moorhouse/pub/planes/>.
- [27] OVCHINNIKOV, P.: *Automorphisms of the poset of skew projections*, J. Funct. Anal. **115** (1993), 184–189.
- [28] PTÁK, P.—PULMANNOVÁ, S.: *Orthomodular Structures as Quantum Logics*. Fundam. Theor. Phys. 44, Kluwer, Dordrecht, 1991.
- [29] SULTANBEKOV, F.: *On (3, 3)-homogeneous Greechie orthomodular posets*, Internat. J. Theoret. Phys. **44** (2005), 957–963.
- [30] ULHORN, U.: *Representation of symmetry transformations in quantum mechanics*, Ark. Fys. **23** (1963), 307–340.

Received 12. 2. 2014  
Accepted 21. 5. 2014

*\*Physical Sciences Laboratory  
New Mexico State University  
Las Cruces, NM 88003  
USA  
E-mail: thannan@nmsu.edu*

*\*\*Department of Mathematical Sciences  
New Mexico State University  
Las Cruces, NM 88003  
USA  
E-mail: jharding@nmsu.edu*