KYBERNETIKA — VOLUME *56* (2020), NUMBER 5, PAGES 934–947

A NOTE ON REPRESENTING DOWLING GEOMETRIES BY PARTITIONS

František Matúš and Aner Ben-Efraim

We prove that a rank $\geqslant 3$ Dowling geometry of a group H is partition representable if and only if H is a Frobenius complement. This implies that Dowling group geometries are secret-sharing if and only if they are multilinearly representable.

Keywords: matroid representations, partition representations, Dowling geometries, Frobenius groups

Classification: 05B35

1. INTRODUCTION

The Dowling group geometeries [5] is a class of matroids defined for every finite group H and for every rank $n \in \mathbb{N}$. When $n \geqslant 3$, the matroid circuits are determined by the group structure and non-isomorphic groups result in non-isomorphic matroids.[1]

The connection between the representability of the Dowling group geometry and the underlying group was observed already in Dowling's seminal work [5]: Dowling showed that, for $n \geqslant 3$, the matroid is linearly representable if and only if the underlying group is cyclic. Later works showed connections between the underlying group and other types of matroid representability: multilinear representability [1, 12], skew-partial field representability [12, 16], and representability over rings [16]. In particular, for $n \geqslant 3$, the Dowling group geometry is multilinearly representable, skew-partial field representable, and representable over some ring if and only if the group is fixed-point free, or equivalently a Frobenius complement.[2]

Dowling group geometries are often used, either by themselves or as building blocks, for separating matroid classes induced by various representation types. For example, Beimel et al. [1] showed that for every prime p, there exists a Dowling geometry that is p-linearly representable, but not ℓ-linearly representable for every $\ell < p$. The Dowling group geometry of the quaternion group has been used, as a building block, by Pendavingh and van Zwam [12] to show a multilinear matroid not representable even over a skew-field, and by Ben-Efraim [2] to show a multilinear matroid that is not algebraic.

DOI: 10.14736/kyb-2020-5-0934

[1] The discussion for $n \leqslant 2$, where the group structure does not affect the matroid structure, is usually omitted.

[2] see Remark 2.1 for a clarification of the definition.

In this work we focus on partition representations, which have received considerable and increasing interest in the last couple of decades. These representations are motivated by questions from cryptography and coding theory, due to their close relation to ideal perfect secret-sharing schemes [3, 14]. Partition representable matroids are also known as almost affinely representable matroids [14], entropic, and secret-sharing matroids [3, 13], and have also been studied in [8]. Simonis and Ashikmin [14] showed that multilinear representability implies partition representability, and that partition representable matroids are minor closed. Some techniques for proving matroids are not partition representable were presented by Seymour [13] and Matúš [8], but this class of matroids is still far from being completely understood.

Our result. In this work we investigate which Dowling group geometries are partition representable. In particular, we show that for $n \geqslant 3$, the Dowling geometry of a group H is partition representable if and only if H is a Frobenius complement. The first direction follows by combining the known results stated above: if H is a Frobenius complement then its Dowling group geometry is multilinear and therefore partition representable.

In contrast, the other direction is non-trivial. It is a long-standing open question whether every partition representable matroid is multilinearly representable [8, 14], and many conjecture that this is not the case. Beimel et al. [1] proved that if the Dowling geometry is multilinearly representable then H is a Frobenius complement, by relying on results from linear algebra. Additionally, Dowling group geometries are often used to separate classes induced by different representation types. Thus, for groups that are not Frobenius complements, the Dowling group geometries were natural candidates for a partition representable, non-multilinear matroid. However, in this work we prove that these matroids are not partition representable as well. Thus, the Dowling group geometries are partition representable if and only if they are multilinearly representable.

Open questions. In this work we classify the Dowling group geometries that are partition representable. Another representation type that is often of interest is algebraic representations, but not much is known about algebraic representations of the Dowling group geometries: since linearly representable matroids are algebraic, Dowling geometries of cyclic groups are algebraic. Additionally, a construction by Evans and Hrushovski [6] involving elliptic curves shows that the Dowling geometries of some non-cyclic groups are algebraic, e.ġ., the Dowling geometries of $\mathrm{SL}(2,3)$ and of the quaternion group are algebraic in characteristic 2, and the Dowling geometry of the group $C_3 \rtimes C_4$ is algebraic in characteristic 3; we observe that these three groups are Frobenius complements. On the other hand, there are no groups for which it is known that the Dowling group geometry is not algebraic. Classifying the algebraic Dowling group geometries seems an intriguing open problem.

There are also many interesting open questions on partition representable matroids. For example, it is not known whether the dual of a partition representable matroid is also partition representable. It is not even known whether there exists a partition representable, non-multilinear matroid. Following our result, if such a matroid exists, it cannot be a Dowling group geometry.

Organization. In Section 2 we give the definitions of the rank-3 Dowling group geometry and of partition representations, and present some useful notation, terminology, and observations. Section 3 contains our main theorem and the beautiful proof written by Fero Matúš. In order to avoid making significant changes to this proof, which is written in Fero's uncompromising style, Appendix A contains further expansions and explanations for marked paragraphs in the proof.

2. PRELIMINARIES

We assume the reader is familiar with the basic concepts of matroid theory, such as circuits, minors, linear representations, etc. A good introduction to matroid theory is [10].

Remark 2.1. We clarify the definition of Frobenius complement that we use in this paper: Let G be a finite group and H a non-trivial subgroup of its automorphism group, i. e., $\{\iota\} \neq H \leqslant \mathsf{Aut}(G)$. The subgroup H is a *subgroup of fixed-point free automorphisms*, if each non-identity automorphism in H does not fix any element of G except the identity, i. e., $\forall \iota \neq \varphi \in H, \forall 1 \neq g \in G, \varphi(g) \neq g$. It is known (see for example [11, Chapter 3] or [7, Theorem 25.5]) that this is equivalent to H being a *Frobenius complement* and to H being a *fixed-point free group*. Hence, we use these terms interchangeably, even though the standard definitions for these terms are different. We note that Beimel et al. [1] used the standard definition of a fixed-point free group in their proof.

2.1. Dowling group geometries

Dowling introduced the Dowling group geometries in [5]. The Dowling group geometry $Dow_n(H), n \geqslant 1$ is a matroid of rank n constructed from a finite group $(H, \cdot, e)$ on a ground set with $n + \binom{n}{2}|H|$ points [5]. For our main theorem we require only the definition of $Dow_3(H)$, which we give below. The formal definition of $Dow_n(H)$ for general n can be found in [5] and [10].

Definition 2.2. The ground set of $Dow_3(H)$ consists of three joints $\mathsf{1}$, $\mathsf{2}$, $\mathsf{3}$ and three disjoint copies of H, which we denote by H, $\dot{H}$ and $\ddot{H}$. It is a simple paving matroid whose lines with at least three points are either the edges

$$\{\mathsf{1},\mathsf{2}\} \cup H\,, \qquad \{\mathsf{2},\mathsf{3}\} \cup \dot{H} \qquad \text{and} \qquad \{\mathsf{3},\mathsf{1}\} \cup \ddot{H}\,,$$

or $\{h, \dot{k}, \ddot{l}\}$ for $h, k, l \in H$ such that $lkh = e$; here, $\dot{k} \in \dot{H}$ and $\ddot{l} \in \ddot{H}$ are copies of k, l. The rank of every set with $\geqslant 3$ elements is 2 if it is contained in a line above, and 3 otherwise.

Example 2.3. The case $H = C_2 = \{e, h\}$ is depicted in Figure 1.

2.2. Partition representations of matroids

We follow [8] and present the definition of partition representations and some useful notation and observations. A more detailed coverage of partition representations can be found in [8]. The definition of a partition representable matroid is as follows:

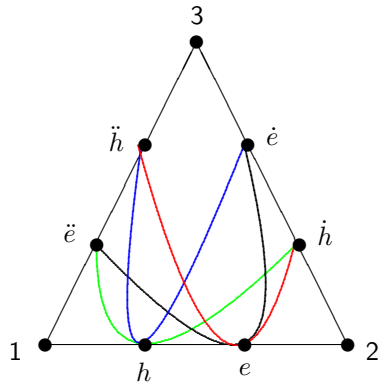

Fig. 1. Geometric representation of $Dow_3(C_2)$.

Definition 2.4. Let $M = (E, r)$ be a matroid with rank function r. The matroid is *partition representable* if there exist an integer $d \geqslant 2$, a finite set Ω of cardinality $|\Omega| = d^{r(E)}$, and partitions $(\xi_i)_{i\in E}$ of Ω, such that for every $I \subset E$, the meet-partition[3] $\xi_I \triangleq \bigwedge_{i\in I} \xi_i$ has $d^{r(I)}$ blocks, all of the same cardinality. The set of partitions is called the *partition representation*.

Observe that all the blocks of ξ_I have cardinality $d^{r(E)-r(I)}$. In particular, $\xi_\emptyset$ has only one block being the whole set Ω, and ξ_E has $|\Omega|$ blocks, being the singletons of Ω.

Example 2.5. Let $G = \{0, 1\}$, $d = |G| = 2$, and $\Omega = G \times G$. Denote the partitions $\xi_1 = \{G \times \{g\} | g \in G\}$, $\xi_2 = \{\{g\} \times G | g \in G\}$, and $\xi_3 = \{\{(0,0),(1,1)\},\{(0,1),(1,0)\}\}$. Note that all the partitions have $2{=}d^1$ blocks of the same size and all the meet partitions $\xi_1 \wedge \xi_2$, $\xi_2 \wedge \xi_3$, $\xi_1 \wedge \xi_3$, and $\xi_1 \wedge \xi_2 \wedge \xi_3$ are equal and have $4 = d^2$ blocks. Hence, (ξ_1, ξ_2, ξ_3) is a partition representation of $\mathsf{U}_{2,3}$.

Partition representable matroids have been studied in several works, e. g., [3, 8, 14, 13], also under the names almost affinely representable and secret-sharing matroids. In particular, [14] showed that all multilinearly representable matroids are partition representable. A basic concept in partition representations is *isotopy*.

Definition 2.6. Two partition representations $(\xi)_{i\in E}$ and $(\eta)_{i\in E}$ of a matroid $M = (E, r)$, which partition the sets Ω_ξ and Ω_η, respectively, are called *isotopic* if there exists a bijection $f\colon \Omega_\xi \to \Omega_\eta$ such that $\forall i \in E, f(\xi_i) = \eta_i$.

Isotopic partition representations are considered equivalent. Hence, as explained in [8], one can to look at Ω as an n-ary Cartesian power of a set G of cardinality d, where $n = r(E)$. Furthermore, one can choose a base of the matroid and set its corresponding

[3]The *meet-partition* of a set of partitions is the coarsest partition refining each of the partitions in the set.

partitions to be $\{G^i \times \{g\} \times G^{n-i-1} | g \in G\}_{i\in[n]}$, so each block of the ith partition is of the form $G^i \times \{g\} \times G^{n-i-1}$ for some $g \in G$.

For example, if $Dow_3(H)$ is partition representable then $|\Omega| = d^3$ for some integer $d \geqslant 2$, and we may assume $\Omega = G \times G \times G$ for some G of size d. Further, we can choose the base $\{1, 2, 3\}$, i. e., the set of joints, and set its corresponding partitions ξ_1,ξ_2, and ξ_3 to have the blocks $\{g\}\times G\times G$, $G\times\{g\}\times G$, and $G\times G\times\{g\}$, respectively.

A partition ρ of $\Omega = G \times G$ is called a *Latin partition* if there exists a quasigroup operation $\circ$ on G such that the blocks of the partition are $\{(x, y)|x \circ y = a\}_{a\in G}$, i. e., each block consists of all the pairs that map to the same quasigroup element.[4] In Example 2.5, ξ_3 is a Latin partition by the group operation of addition modulo 2. On the other hand, ξ_1 and ξ_2 are not Latin partitions, since in any quasigroup if $g, h_1, h_2 \in G$ and $h_1 \neq h_2$ then $g \circ h_1 \neq g \circ h_2$ and $h_1 \circ g \neq h_2 \circ g$. Therefore, in any Latin partition of $G \times G$, each block contains d couples such that each $g \in G$ occurs exactly once in the first coordinate of a couple and exactly once in the second coordinate of a couple.

Two Latin partitions ρ and π of $\Omega = G \times G$ corresponding to quasigroup operations $\circ$ and $\cdot$, respectively, are termed *orthogonal* if the mapping $(x, y) \to (x \circ y, x \cdot y)$ is bijective.[4] Note that this implies that the blocks of the meet partition $\rho \wedge \pi$ are the singletons.

Example 2.7. Let $\Omega = G \times G$, where G is a set of size $d \geqslant 2$, and assume that $\xi_1 = \{\{g\} \times G|g \in G\}$, $\xi_2 = \{G \times \{g\}|g \in G\}$, and ξ_3 and ξ_4 are orthogonal Latin partitions of Ω. Then it is not difficult to see that $\boldsymbol{\xi} = (\xi_1, \xi_2, \xi_3, \xi_4)$ is a partition representation of $\mathsf{U}_{2,4}$.

If H is a fixed-point free group of automorphisms of G, then the above example can be extended to $\mathsf{U}_{2,|H|+2}$.

Lemma 2.8. Let $\Omega = G \times G$, where G is a group of size $d \geqslant 2$, and let $H \leqslant \mathsf{Aut}(G)$ be a subgroup of fixed-point free automorphisms. Then $\boldsymbol{\rho}^H = \{\rho_1, \rho_2, (\rho_h)_{h\in H}\}$, where $\rho_1 = \{\{g\} \times G|g \in G\}$, $\rho_2 = \{G \times \{g\}|g \in G\}$, and

$$\rho_h = \{\{(x, ah(x))|x \in G\}|a \in G\},$$

is a partition representation of $\mathsf{U}_{2,|H|+2}$.

P r o o f. Clearly, every single partition has $|G|$ blocks of size $|G|$. Thus, it remains to prove that the meet partition of every 2 elements has $|G|^2$ blocks, i. e., to show that the blocks of the meet-partition are the singletons. We show this for $\rho_{h_1} \wedge \rho_{h_2}$, leaving the cases with ρ_1 and ρ_2 as exercise.

Assume that (x_1, y_1) and (x_2, y_2) are two distinct elements that belong to the same block in $\rho_{h_1} \wedge \rho_{h_2}$, with $h_1 \neq h_2$. This implies that they are in the same block in ρ_{h_1} so $y_1 = a_1h_1(x_1)$, $y_2 = a_1h_1(x_2)$ for some $a_1 \in G$. Additionally, they are in the same block in ρ_{h_2} so $y_1 = a_2h_2(x_1)$ and $y_2 = a_2h_2(x_2)$ for some $a_2 \in G$.

Using the equations on y_1, we get $a_1^{-1}a_2 = h_1(x_1)h_2(x_1)^{-1}$. Similarly, $a_1^{-1}a_2 = h_1(x_2)h_2(x_2)^{-1}$ using the equations on y_2. So, $h_1(x_2)^{-1}h_1(x_1) = h_2(x_2)^{-1}h_2(x_1)$, and

[4]The definition of (orthogonal) Latin partitions can also be extended to $\Omega = G^n$ for any n, cf. [8].

using that h_1, h_2 are homomorphisms, we get $h_1(x_2^{-1}x_1) = h_2(x_2^{-1}x_1)$. Now applying h_2^{-1} on both sides, and using that h_1, h_2 are automorphisms, we receive $h_2^{-1}h_1(x_2^{-1}x_1) = x_2^{-1}x_1$, but as H is fixed-point free this implies that either $h_2^{-1}h_1 = \iota$ or $x_2^{-1}x_1 = 1_G$. The first case implies $h_1 = h_2$, a contradiction. In the second case we get that $x_1 = x_2$ and $y_1 = a_1h_1(x_1) = a_1h_1(x_2) = y_2$, so $(x_1, y_1) = (x_2, y_2)$, a contradiction. □

We end this section with a few more notations. If ρ is a partition of $G \times G$ and $B \in \rho$ is a block, we can look at the block transposition $B^{tr} = \{(y, x)|(x, y) \in B\}$. A partition is transposed by transposing all the blocks – note that the number of blocks in ρ^{tr} and their size are equal to those of ρ.

Suppose ρ_1, ρ_2, and ρ_3 are three partitions $\Omega = G \times G$ and that $B \in \rho_1$, $C \in \rho_2$, and $D \in \rho_3$ are blocks. Then we can look at the set $\overline{BCD} \triangleq \{(x, y, z)|(x, y) \in B, (y, z) \in C, (z, x) \in D\}$ of $G \times G \times G$. Note that this set might be empty, for example, if $B = C = \{(x, x)|x \in G\}$ then $\overline{BCD}$ is non-empty if and only if $(x, x) \in D$ for some $x \in G$ as well. Choosing the correct blocks and finding the conditions when this set is non-empty plays an important role in our main proof.

2.3. Partition representations of Dowling geometries

All matroids of rank $\leqslant 2$ are linearly representable. Hence, for $n \leqslant 2$ the Dowling matroids are linearly representable and therefore partition representable. For $n \geqslant 3$, if H is fixed-point free then $Dow_n(H)$ is multilinearly representable [1, 16], and therefore also partition representable [14]. We note that $Dow_3(\{e\}) \cong M(K_4)$, i. e., the rank-3 Dowling geometry of the trivial group is isomorphic to the cycle matroid of the clique on four vertices, and the partition representations of this matroid have been fully classified in [8].

Lemma 2.9. (Matúš [8, Proposition 3.1]) Every partition representation of $M(K_4)$ is isotopic to the system of partitions,

$$\boldsymbol{\rho}^{(G,\cdot)} \triangleq \left(\rho_1^{(G,\cdot)}, \rho_2^{(G,\cdot)}, \rho_3^{(G,\cdot)}, \rho_4^{(G,\cdot)}, \rho_5^{(G,\cdot)}, \rho_6^{(G,\cdot)}\right), \tag{1}$$

constructed from a finite group $(G, \cdot)$, where the blocks of $\rho_1^{(G,\cdot)}$, $\rho_2^{(G,\cdot)}$ and $\rho_3^{(G,\cdot)}$ are $\{g\} \times G \times G$, $G \times \{g\} \times G$, and $G \times G \times \{g\}$, respectively, and

$$\begin{aligned}
\rho_4^{(G,\cdot)} &\triangleq \{\{(x, y, z)|xy^{-1} = a\}|a \in G\} \\
\rho_5^{(G,\cdot)} &\triangleq \{\{(x, y, z)|yz^{-1} = a\}|a \in G\} \\
\rho_6^{(G,\cdot)} &\triangleq \{\{(x, y, z)|zx^{-1} = a\}|a \in G\}.
\end{aligned}$$

Two partition representations $\boldsymbol{\rho}^{(G,\cdot)}$ and $\boldsymbol{\rho}^{(G',\circ)}$ are isotopic if and only if the groups $(G, \cdot)$ and $(G', \circ)$ are isomorphic.

Thus, our result can be seen as extension of [8, Proposition 3.1] to general groups and higher ranks. For the rest of this paper, unless explicitly stated, we assume H is non-trivial. As a warm-up to our main theorem, which we present in Section 3, we next show

that the Dowling geometry $Dow_3(H)$ of the Frobenius complement H in a Frobenius group Γ can be represented by the partitions in Figure 2: The corresponding partition representation

$$\boldsymbol{\pi}^{\Phi} \triangleq \left(\pi_1, \pi_2, \pi_3, (\pi_h)_{h\in H}, (\pi_{\dot{k}})_{k\in H}, (\pi_{\ddot{l}})_{l\in H}\right)$$

lives on $\Omega = G^3$, where G is the Frobenius kernel of Γ. The mappings Φ_h are the conjugations, $\{\Phi_h\colon g \mapsto h^{-1}gh\}_{h\in H}$, which are fixed-point-free automorphisms of G. The mapping $\Phi\colon h \mapsto \Phi_h$ is a monomorphism of H into $\mathsf{Aut}(G)$, so H can be identified with a subgroup of fixed-point free automorphisms. As we shall see in Section 3, every partition representation of $Dow_3(H)$ is in fact isotopic to this type of partition representation.

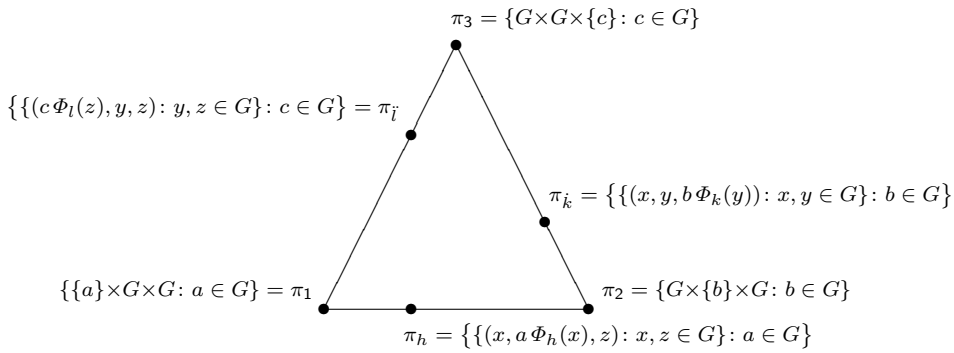

Fig. 2. A partition representation $\boldsymbol{\pi}^{\Phi}$ of $Dow_3(H)$ for a Frobenius complement H in Γ lives on the cube G^3 of the Frobenius kernel G to H.

Lemma 2.10. The set of partitions $\boldsymbol{\pi}^{\Phi}$ define a partition representation of $Dow_3(H)$.

P r o o f . First, as $Dow_3(H)$ is rank 3 and paving, it follows from [8, Lemma 1.4] that it suffices to check the subsets of size 3. The subsets of size 3 can be classified into 4 types – 2 types of bases and 2 types of circuits:

1. Circuits where all 3 points are on the same edge,
2. Bases where exactly 2 of the points are on the same edge,
3. Circuits where each point is on a different edge, corresponding to $h_1, \dot{h}_2, \ddot{h}_3$, such that $h_3h_2h_1 = e$.
4. Bases where each point is on a different edge, corresponding to $h_1, \dot{h}_2, \ddot{h}_3$, such that $h_3h_2h_1 \neq e$.

Therefore, it remains to show that the meet partitions of types 1 and 3 have $|G|^2$ blocks of size $|G|$ and the meet partitions of types 2 and 4 have $|G|^3$ blocks of size 1. For type 1 this follows from Lemma 2.8, because the additional coordinate is free. We next

show for types 2, 3, and 4, where for simplicity in type 2 we consider only the subsets not containing any of the joints.

Suppose the set is of type 2, with the points h_1, h_2 being on the first edge and the point $\dot{h}_3$ on the second egde, with corresponding partitions ξ_{h_1},ξ_{h_2}, and $\xi_{\dot{h}_3}$. From Lemma 2.8, the blocks of the meet partition ξ_{h_1,h_2} are of the form $\{g\} \times \{k\} \times G$ for g, k running over G. Therefore, the blocks of the meet partition $\xi_{h_1,h_2,\dot{h}_3}$ are the singletons $\{g\} \times \{k\} \times \{l\}$ for g, k, l running over G – any coarser partition that contains a non-singleton block in the first 2 coordinates is not contained in any block of ξ_{h_1,h_2}, but fixing the second coordinate corresponds to a unique block in $\xi_{\dot{h}_3}$ for each choice of the 3rd coordinate. The other subsets of type 2 follow from symmetric arguments.

Now suppose the set is of type 3, with the points $h_1, \dot{h}_2, \ddot{h}_3$ being on the first, second, and third edge respectively, with corresponding partitions ξ_{h_1},$\xi_{\dot{h}_2}$, and $\xi_{\ddot{h}_3}$. Then the blocks of the meet partition $\xi_{h_1,\dot{h}_2}$ are of the form

$$\{(g, a\Phi_{h_1}(g), b\Phi_{h_2}(a\Phi_{h_1}(g))) \colon g \in G\}$$

For a, b running over G. Looking at the partition $\xi_{\ddot{h}_3}$, we see the blocks of the meet partition $\xi_{h_1,\dot{h}_2,\ddot{h}_3}$ are of the form

$$\{(g, a\Phi_{h_1}(g), b\Phi_{h_2}(a\Phi_{h_1}(g))) \colon g \in G,\ g = c\Phi_{h_3}(b\Phi_{h_2}(a\Phi_{h_1}(g)))\}$$

for a, b, c running over G. Note that

$$c\Phi_{h_3}(b\Phi_{h_2}(a\Phi_{h_1}(g))) = c\Phi_{h_3}(b)\Phi_{h_3h_2}(a)\Phi_{h_3h_2h_1}(g).$$

Furthermore, $h_3h_2h_1 = e$, so $\Phi_{h_3h_2h_1} = \iota$, the identity function. This simplifies the additional condition to

$$c\Phi_{h_3}(b)\Phi_{h_3h_2}(a) = e.$$

We observe that for every choice of $a, b \in G$, there exists a unique $c \in G$ satisfying the condition, and this holds for all $g \in G$. Thus, we have $|G|^2$ blocks of size $|G|$. The other subsets of type 3 follow from symmetric arguments.

Now suppose the set is of type 4, with the points $h_1, \dot{h}_2, \ddot{h}_3$ being on the first, second, and third edge respectively, with corresponding partitions ξ_{h_1},$\xi_{\dot{h}_2}$, and $\xi_{\ddot{h}_3}$. Following the previous case, we again get that the meet partitions $\xi_{h_1,\dot{h}_2,\ddot{h}_3}$ are of the form

$$\{(g, a\Phi_{h_1}(g), b\Phi_{h_2}(a\Phi_{h_1}(g))) \colon g \in G,\ g = c\Phi_{h_3}(b)\Phi_{h_3h_2}(a)\Phi_{h_3h_2h_1}(g)\}$$

for a, b, c running over G. This time, however, we have $h_3h_2h_1 \neq e$, so $\Phi_{h_3h_2h_1} \neq \iota$. Therefore, by the assumption, $\Phi_{h_3h_2h_1}$ is fixed-point free, so it is an orthomorphism, i. e., $g \mapsto \Phi_{h_3h_2h_1}(g)g^{-1}$ is a permutation of G. So for each choice of $a, b, c \in G$ there exists a unique g such that the condition $g = c\Phi_{h_3}(b)\Phi_{h_3h_2}(a)\Phi_{h_3h_2h_1}(g)$ holds. Therefore, there are $|G|^3$ singleton blocks. The other subsets of type 4 follow from symmetric arguments. □

Note that if $\Phi_{h_3h_2h_1}$ is not fixed-point free for some $h_1, h_2, h_3 \in H$ for which $h_3h_2h_1 \neq e$, then the above arguments fail and we do not get a legal partition representation.

3. MAIN THEOREM

As we have seen, if H is a fixed-point free group, then $Dow_n(H)$ is partition representable. In this section, we shall show that the converse is also true, i. e., if $Dow_n(H)$ for $n \geqslant 3$ is partition representable, then H is fixed-point free. We first note that for $n \geqslant 3$, the matroid $Dow_n(H)$ contains $Dow_3(H)$ as a minor by restriction (see for example [10, Chapter 6.10]). Therefore, if $Dow_3(H)$ is not partition representable, then neither is $Dow_n(H)$. Thus, it suffices to look only at $Dow_3(H)$. We now present and prove our main theorem.

Theorem 3.1. If $Dow_3(H)$ constructed from a group $(H, \cdot, e)$ has a partition representation (with order $d \geqslant 2$), then there exists a group $(G, \circ, 1)$ with d elements such that $\mathsf{Aut}(G)$ contains an isomorphic copy of H that is fixed-point free.

In the following proof, only minimal changes have been made to Fero's original proof. Therefore, the proof is succinct, in accordance with his uncompromising style. For the benefit of the readers, we provide several expansions with additional explanations in Appendix A, marked after the relevant paragraphs.

Proof. Let $\boldsymbol{\xi} = \big(\xi_1, \xi_2, \xi_3, (\xi_h)_{h\in H}, (\xi_{\dot{k}})_{k\in H}, (\xi_{\ddot{l}})_{l\in H}\big)$ be a configuration representing $Dow_3(H)$ and having degree $d \geqslant 2$. Up to an isotopy, it can be assumed that $\boldsymbol{\xi}$ lives on a set $\Omega = G^3$ where G is a set with d elements, and that the blocks of $\xi_1/\xi_2/\xi_3$ are of the form

$$\{g\}\times G\times G \;/\; G\times\{g\}\times G \;/\; G\times G\times\{g\},\ g \in G.$$

Since $h \in H$ is on the line through $\{1, 2\}$, there exists a Latin partition ρ_h of $G\times G$ such that the blocks of ξ_h have the form $B\times G$, $B \in \rho_h$.[A.1] This means that B consists of d couples such that each $g \in G$ occurs in the first coordinate of a couple and in the second coordinate of a couple. Hence, for a unique permutation $\phi_{h,B}$ of G

$$B = \{(\phi_{h,B}(y), y)\colon y \in G\}\,, \qquad B \in \rho_h\,.$$

Analogously, the blocks of $\xi_{\dot{h}}$ are $G\times C$ where the blocks $C = \{(\phi_{\dot{h},C}(z), z)\colon z \in G\}$ form a Latin partition $\rho_{\dot{h}}$, and the blocks of $\xi_{\ddot{h}}$ are $\{(x, g, \phi_{\ddot{h},D}(x))\colon x, g \in G\}$ where $D = \{(\phi_{\ddot{h},D}(x), x)\colon x \in G\}$ are blocks of a Latin partition $\rho_{\ddot{h}}$.

The restriction of $Dow_3(H)$ to $\{1, 2, 3, e, \dot{e}, \ddot{e}\}$ is $\mathsf{M}(K_4)$. By Lemma 2.9, the set G can be endowed with a group operation $\circ$, such that, up to isotopy, the blocks of $\xi_e/\xi_{\dot{e}}/\xi_{\ddot{e}}$ are $\Delta_a \times G \;/\; G \times \Delta_a \;/\; \{(y, g, x)\colon (x, y) \in \Delta_a,\ g \in G\}$ where

$$\Delta_a = \{(x, y)\colon x \circ y^{\circ -1} = a\}\,, \qquad a \in G\,.$$

Here, $y^{\circ -1}$ is the inverse of y in the operation $\circ$ on G. Let σ denote the partition of $G\times G$ with the blocks Δ_a, $a \in G$. Then, $\rho_e = \rho_{\dot{e}} = \rho_{\ddot{e}} = \sigma$ and $\phi_{e,\Delta_a} = \phi_{\dot{e},\Delta_a} = \phi_{\ddot{e},\Delta_a}$ which is the mapping $y \mapsto a \circ y$, $y \in G$. In particular, $\phi_{e,\Delta_1} = \iota$.

Let $lkh = e$ for $h, k, l \in H$, and $B \in \rho_h$, $C \in \rho_{\dot{k}}$ and $D \in \rho_{\ddot{l}}$. If the block

$$\overline{BCD} = \{(x, y, z)\colon (x, y) \in B,\ (y, z) \in C,\ (z, x) \in D\}$$

of $\xi_h \wedge \xi_{\dot{k}} \wedge \xi_{\ddot{l}}$ is nonempty then it contains d triples (x, y, z) because $h, \dot{k}, \ddot{l}$ are collinear so that $\xi_h \wedge \xi_{\dot{k}} \wedge \xi_{\ddot{l}}$ has d^2 blocks. Therefore,

$$\phi_{h,B} \bullet \phi_{\dot{k},C} \bullet \phi_{\ddot{l},D} = \iota \,.^{[A.2]} \tag{2}$$

Recall that the transposition of a subset A of $G \times G$ is $A^{\mathrm{tr}} = \{(x, y) \colon (y, x) \in A\}$, and the partitions are transposed by transposing all blocks, e. g., σ is self-transposed.

The choice $h^{-1}eh = e$, $B \in \rho_{h^{-1}}$, $\Delta_1 \in \rho_{\dot{e}}$ and $D \in \rho_{\ddot{h}}$ renders

$$\overline{B\Delta_1 D} = \{(x, y, y) \colon (x, y) \in B,\ (y, x) \in D\}$$

nonempty if and only if $D = B^{\mathrm{tr}}$.[A.3] Hence, $\rho^{\mathrm{tr}}_{h^{-1}} = \rho_{\ddot{h}}$ and (2) reduces to

$$\phi_{h^{-1},B} \bullet \iota \bullet \phi_{\ddot{h},B^{\mathrm{tr}}} = \iota \,, \qquad h \in H,\ B \in \rho_{h^{-1}} \,.$$

Similarly, the choice $h^{-1}he = e$, $B \in \rho_{h^{-1}}$, $C \in \rho_{\dot{h}}$ and $\Delta_1 \in \rho_{\dot{e}}$ renders

$$\overline{BC\Delta_1} = \{(x, y, x) \colon (x, y) \in B,\ (y, x) \in C\}$$

nonempty if and only if $C = B^{\mathrm{tr}}$. Hence, $\rho^{\mathrm{tr}}_{h^{-1}} = \rho_{\dot{h}}$ and

$$\phi_{h^{-1},B} \bullet \phi_{\dot{h},B^{\mathrm{tr}}} \bullet \iota = \iota \,, \qquad h \in H,\ B \in \rho_{h^{-1}} \,.$$

Third choice $eh^{-1}h = e$, $\Delta_1 \in \rho_e$, $B \in \rho_{\dot{h}^{-1}}$ and $D \in \rho_{\ddot{h}}$ renders

$$\overline{\Delta_1 BD} = \{(x, x, y) \colon (x, y) \in B,\ (y, x) \in D\}$$

nonempty if and only if $D = B^{\mathrm{tr}}$. Hence, $\rho^{\mathrm{tr}}_{\dot{h}^{-1}} = \rho_{\ddot{h}}$ and

$$\iota \bullet \phi_{\dot{h}^{-1},B} \bullet \phi_{\ddot{h},B^{\mathrm{tr}}} = \iota \,, \qquad h \in H,\ B \in \rho_{\dot{h}^{-1}} \,.$$

It follows that if $h \in H$ then $\rho_h = \rho_{\dot{h}} = \rho_{\ddot{h}} = \rho^{\mathrm{tr}}_{h^{-1}}$ and thus

$$\phi_{h,B} = \phi_{\dot{h},B} = \phi_{\ddot{h},B} = \phi^{-1}_{h^{-1},B^{\mathrm{tr}}} \,, \qquad\qquad B \in \rho_h \,, \tag{3}$$

known previously only for $h = e$. Then, (2) supplemented with quantification rewrites to

$$\phi_{h,B} \bullet \phi_{k,C} \bullet \phi_{l,D} = \iota \,, \qquad lkh = e,\ B \in \rho_h,\ C \in \rho_k,\ D \in \rho_l \text{ s.t. } \overline{BCD} \neq \emptyset \,. \tag{4}$$

Given a partition ρ_h of $G \times G$ let $A(h)$ denote its block containing the couple $(1, 1)$. Then $A(h)^{\mathrm{tr}} = A(h^{-1})$ as $\rho_h = \rho^{\mathrm{tr}}_{h^{-1}}$.

Let $\Phi \colon h \mapsto \phi^{-1}_{h,A(h)}$ map H to the set of permutations of G. Since $(1, 1, 1)$ belongs to any $\overline{A(h)A(k)A(l)}$,

$$\begin{aligned} \Phi_{hk} = \phi^{-1}_{hk,A(hk)} &\overset{(4)}{=} \phi_{h^{-1},A(h^{-1})} \bullet \phi_{k^{-1},A(k^{-1})} = \phi_{h^{-1},A(h)^{\mathrm{tr}}} \bullet \phi_{k^{-1},A(k)^{\mathrm{tr}}} \\ &\overset{(3)}{=} \phi^{-1}_{h,A(h)} \bullet \phi^{-1}_{k,A(k)} = \Phi_h \bullet \Phi_k \,, \qquad\qquad h, k \in H \,, \end{aligned}$$

using (4) with $k^{-1}h^{-1}(hk) = e$ and (3).[A.4] Thus, Φ is a group homomorphism.

Let $h \in H$. To prove that Φ_h is an automorphism of G, let $x \in G$ and D be the block of $\rho_{h^{-1}}$ that contains $(x^{\circ 1}, 1)$. Then

$$\overline{A(h)\Delta_x D} = \{(y, \phi_{h,A(h)}(y), x^{\circ 1} \circ \phi_{h,A(h)}(y)) \colon y \in G, \ldots \in D\}$$

contains $(1, 1, x^{\circ 1})$. Let $z = z_x = [\phi^{-1}_{h,A(h)}(x^{\circ 1})]^{\circ 1}$. Then

$$\overline{\Delta_z A(h) D} = \{(y, z^{\circ 1} \circ y, \phi_{h,A(h)}(z^{\circ 1} \circ y) \colon y \in G, \ldots \in D\}$$

contains $(1, z^{\circ 1}, x^{\circ 1})$. It follows that the mappings

$$y \mapsto \phi^{-1}_{h,A(h)}(x \circ y) \qquad \text{and} \qquad y \mapsto z_x \circ \phi^{-1}_{h,A(h)}(y)$$

are identical. When $y = 1$ this specializes to $\phi^{-1}_{h,A(h)}(x) = z_x$. Thus,

$$\Phi_h(x \circ y) = \phi^{-1}_{h,A(h)}(x \circ y) = \phi^{-1}_{h,A(h)}(x) \circ \phi^{-1}_{h,A(h)}(y) = \Phi_h(x) \circ \Phi_h(y)\,, \quad x, y \in G\,.[A.5]$$

If $h \neq e$ then the restriction of $Dow_3(H)$ to $\{1, 2, e, h\}$ is $\mathsf{U}_{2,4}$. Then, $\rho_e \neq \rho_h$ implies that Φ is injective. It remains to prove that Φ_h is an orthomorphism.[A.6] As any blocks $B \in \rho_h$ and $\Delta_a \in \rho_e$ intersect in a unique couple, the equation $\phi_{h,B}(g) = a^{\circ 1} \circ g$ has a unique solution $g \in G$. For $B = A(h)$ this recasts to $g = \Phi_h(g)(a^{\circ 1} \circ g)$. This means existence of a unique g such that $a \circ g = \Phi_h(g)$. Thus, $g \mapsto \Phi_h(g) \circ g^{\circ 1}$ is a permutation. □

We are now able to derive our stated result as a corollary from Theorem 3.1 and previously known results.

Corollary 3.2. A rank $\geqslant 3$ Dowling geometry of a non-trivial group H is partition representable if and only if H is a Frobenius complement. This implies that for all n and H, $Dow_n(H)$ is partition representable if and only if it is multilinearly representable.

Proof. For $n \geqslant 3$ and non-trivial H, we recall that $Dow_n(H)$ contains $Dow_3(H)$ as a minor and that partition representations are minor closed. Therefore, if a rank $n \geqslant 3$ Dowling geometry of a group H is partition representable, then so is $Dow_3(H)$. Thus, by Theorem 3.1, H is a subgroup of fixed-point free automorphisms. As explained, this is equivalent to H being a Frobenius complement (see Remark 2.1, or see Remark 3.3 for a direct construction in this case).

In the other direction, we recall that all multilinearly representable matroids are partition representable, and further recall that if H is a Frobenius complement, then $Dow_n(H)$ is multilinearly representable. Hence, if H is a Frobenius complement, then $Dow_n(H)$ is multilinearly representable and therefore partition representable.

Thus, for rank $n \geqslant 3$ and non-trivial H, $Dow_n(H)$ is partition representable if and only if H is a Frobenius complement (equivalently, a fixed-point free group), which matches the characterization for multilinear representability of $Dow_n(H)$ found in [1]. For the trivial cases with $H = \{\iota\}$ or rank $n \leqslant 2$, $Dow_n(H)$ is linearly representable, and therefore both multilinearly and partition representable. □

Remark 3.3. The group $\mathsf{Aut}(G)$ is a subgroup of the symmetric group on G, together with the group $\mathsf{L}(G)$ of left multiplications $x \mapsto gx$, $g \in G$. Then, $\mathsf{L}(G)\mathsf{Aut}(G)$ is a subgroup as well (the holomorph of G, see [9, p. 320]). It contains $\mathsf{L}(G)$ as a normal subgroup and $\mathsf{L}(G) \cap \mathsf{Aut}(G) = \{\iota\}$. In Theorem 3.1, H is embedded in $\mathsf{Aut}(G)$ as Φ_H which is fixed-point-free. Therefore, $\mathsf{L}(G)\Phi_H$ is a Frobenius group, Φ_H is a Frobenius complement and $\mathsf{L}(G)$ its kernel.

ACKNOWLEDGEMENTS

The second author was partially supported by ISF grant 152/17.
Special thanks to anonymous referees for the many helpful suggestions.

(Received April 30, 2019)

REFERENCES

[1] A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin: Multi-linear secret-sharing schemes. Theory Cryptogr. Conf. *14* (2014), 394–418. DOI:10.1007/978-3-642-54242-8_17

[2] A. Ben-Efraim: Secret-sharing matroids need not be Algebraic. Discrete Math. *339* (2015), 8, 2136–2145. DOI:10.1016/j.disc.2016.02.012

[3] E. F. Brickell and D. M. Davenport: On the classification of ideal secret sharing schemes. J. Cryptol. *4* (1991), 73, 123–134. DOI:10.1007/bf00196772

[4] R. Brown: Frobenius groups and classical maximal orders. Memoirs Amer. Math. Soc. *151* (2001), 717. DOI:10.1090/memo/0717

[5] T. A. Dowling: A class of geometric lattices based on finite groups. J. Combinat. Theory, Ser. B *14* (1973), 61–86. DOI:10.1016/s0095-8956(73)80007-3

[6] D. M. Evans and E. Hrushovski: Projective planes in algebraically closed fields. Proc. London Math. Soc. *62* (1989), 3, 1–24. DOI:10.1112/plms/s3-62.1.1

[7] W. Feit: Characters of Finite Groups. W. A. Benjamin Company, Inc., New York 1967.

[8] F. Matúš: Matroid representations by partitions. Discrete Math. *203* (1999), 169–194. DOI:10.1016/s0012-365x(99)00004-7

[9] N. Jacobson: Basic Algebra II. (Second Edition) W. H. Freeman and Co., New York 1989.

[10] J. G. Oxley: Matroid Theory. (Second Edition) Oxford University Press Inc., New York 2011. DOI:10.1093/acprof:oso/9780198566946.001.0001

[11] D. S. Passman: Permutation Groups. Dover Publications, Inc. Mineola, New York 2012.

[12] R. A. Pendavingh and S. H. M. van Zwam: Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. Adv. Appl. Math. *50* (2013), 1, 201–227. DOI:10.1016/j.aam.2011.08.003

[13] P. D. Seymour: On secret-sharing matroids. J. Combinat. Theory, Ser. B *56* (1992), 69–73. DOI:10.1016/0095-8956(92)90007-k

[14] J. Simonis and A. Ashikhmin: Almost affine codes. Designs Codes Cryptogr. *14* (1998), 2, 179–197. DOI:10.1023/a:1008244215660

[15] M. Suzuki: Group Theory I. Springer-Verlag, Berlin 1982.

[16] D. Vertigan: Dowling Geometries representable over rings. Ann. Combinat. *19* (2015), 225–233. DOI:10.1007/s00026-015-0250-4

A. ADDITIONAL EXPLANATIONS AND EXPANSIONS FOR THE PROOF

Explanation A.1. Since $\{1,2,h\}$ is a circuit, by definition the meet partition of $\xi_1 \wedge \xi_2 \wedge \xi_h$ contains d^2 blocks of size d. Therefore, $\xi_1 \wedge \xi_2 \wedge \xi_h = \xi_1 \wedge \xi_2$, which clearly has blocks of the form $\{g_1\} \times \{g_2\} \times G$ for $g_1, g_2 \in G$, and further $\xi_1 \wedge \xi_2 \wedge \xi_h = \xi_2 \wedge \xi_h = \xi_1 \wedge \xi_h$. This implies that there exists a Latin partition ρ_h of $G \times G$ such that the blocks of ξ_h have the form $B \times G$, $B \in \rho_h$.

Expansion A.2. We first note that if $lkh = e$ for $h, k, l \in H$, and $B \in \rho_h$, $C \in \rho_{\dot{k}}$ and $D \in \rho_{\ddot{l}}$, then

$$\overline{BCD} = \{(x,y,z)\colon (x,y) \in B,\ (y,z) \in C,\ (z,x) \in D\}$$

is a block of $\xi_h \wedge \xi_{\dot{k}} \wedge \xi_{\ddot{l}}$. To see this, observe that if a partition refines ξ_h, $\xi_{\dot{k}}$, and $\xi_{\ddot{l}}$ then in each of its blocks all 3 conditions must hold for some $B \in \rho_h$, $C \in \rho_{\dot{k}}$ and $D \in \rho_{\ddot{l}}$. On the other hand, all the non-empty blocks $\overline{BCD}$, for $B \in \rho_h$, $C \in \rho_{\dot{k}}$ and $D \in \rho_{\ddot{l}}$ form a partition of Ω, hence this must be the meet partition.

Next, if $\overline{BCD}$ is nonempty then it contains d triples (x,y,z), because $h, \dot{k}, \ddot{l}$ are collinear, so $\xi_h \wedge \xi_{\dot{k}} \wedge \xi_{\ddot{l}}$ has d^2 blocks. Furthermore, the x in each triple is unique, because B is a block of a Latin partition. Note that in $\overline{BCD}$, by definition, $x = \phi_{h,B}(y)$, $y = \phi_{\dot{k},C}(z)$, and $z = \phi_{\ddot{l},D}(x)$, so $x = \phi_{h,B}(\phi_{\dot{k},C}(\phi_{\ddot{l},D}(x)))$ for all $x \in G$. Therefore, whenever $\overline{BCD}$ is non-empty,

$$\phi_{h,B} \bullet \phi_{\dot{k},C} \bullet \phi_{\ddot{l},D} = \iota\,. \tag{5}$$

Explanation A.3. The choice $h^{-1}eh = e$, $B \in \rho_{h^{-1}}$, $\Delta_1 \in \rho_{\dot{e}}$ and $D \in \rho_{\ddot{h}}$ renders

$$\overline{B\Delta_1 D} = \{(x,y,y)\colon (x,y) \in B,\ (y,x) \in D\}$$

nonempty if and only if $D \cap B^{\mathrm{tr}} \neq \emptyset$. In this case $|B| = |D| \overset{(A.2)}{=} |\overline{B\Delta_1 D}| = |D \cap B^{\mathrm{tr}}|$, so this holds if and only if $D = B^{\mathrm{tr}}$. For every $B \in \rho_{h^{-1}}$, the set $\{(x,y,y)\colon (x,y) \in B\}$ is non-empty, so there exists a block $D \in \rho_h$ such that $\overline{B\Delta_1 D} \neq \emptyset$. Thus, by size considerations, this block is unique and equal to B^{tr}.

Explanation A.4. First, note that $(1,1,1)$ belongs to any $\overline{A(h)A(k)A(l)}$, because $(1,1)$ belongs to all three blocks. Thus, by using (4) with $k^{-1}h^{-1}(hk) = e$ we get

$$\phi_{hk,A(hk)} \bullet \phi_{h^{-1},A(h^{-1})} \bullet \phi_{k^{-1},A(k^{-1})} = \iota \Rightarrow \phi_{h^{-1},A(h^{-1})} \bullet \phi_{k^{-1},A(k^{-1})} = \phi^{-1}_{hk,A(hk)}. \tag{6}$$

Using this and (3) we find that

$$\begin{aligned} \Phi_{hk} = \phi^{-1}_{hk,A(hk)} &\overset{(6)}{=} \phi_{h^{-1},A(h^{-1})} \bullet \phi_{k^{-1},A(k^{-1})} = \phi_{h^{-1},A(h)^{\mathrm{tr}}} \bullet \phi_{k^{-1},A(k)^{\mathrm{tr}}} \\ &\overset{(3)}{=} \phi^{-1}_{h,A(h)} \bullet \phi^{-1}_{k,A(k)} = \Phi_h \bullet \Phi_k\,, \qquad\qquad h,k, \in H\,. \end{aligned}$$

Expansion A.5. Let $h \in H$. To prove that Φ_h is an automorphism of G, fix $x \in G$ and let D be the block of $\rho_{h^{-1}}$ that contains $(x^{\circ\,1}, 1)$. Then

$$\overline{A(h)\Delta_x D} = \{(y, \phi_{h,A(h)}(y), x^{\circ\,1} \circ \phi_{h,A(h)}(y))\colon y \in G,\ (x^{\circ\,1} \circ \phi_{h,A(h)}(y), y) \in D\}$$

contains $(1, 1, x^{\circ\,1})$. Since $\overline{A(h)\Delta_x D}$ is a non-empty block of $\xi_h \wedge \xi_{\dot{e}} \wedge \xi_{\ddot{h}^{-1}}$, it contains d triples, and in particular a triple $(y, \phi_{h,A(h)}(y), x^{\circ\,1} \circ \phi_{h,A(h)}(y))$ for every $y \in G$. Similarly, by setting $z = z_x = [\phi^{-1}_{h,A(h)}(x^{\circ\,1})]^{\circ\,1}$, we find that

$$\overline{\Delta_z A(h) D} = \{(y, z^{\circ\,1} \circ y, \phi_{h,A(h)}(z^{\circ\,1} \circ y)\colon y \in G,\ (\phi_{h,A(h)}(z^{\circ\,1} \circ y), y) \in D\}$$

contains $(1, z^{\circ 1}, x^{\circ 1})$, and so by similar consideration also has size d, i. e., a triple for each $y \in G$. Note that the same block D is used in both cases, and therefore the set of pairs $\{(x^{\circ 1} \circ \phi_{h,A(h)}(y), y)\}_{y \in G}$ and $\{(\phi_{h,A(h)}(z^{\circ 1} \circ y), y)\}_{y \in G}$ are equal. It follows that the mappings

$$y \mapsto \phi^{-1}_{h,A(h)}(x \circ y) \qquad \text{and} \qquad y \mapsto z_x \circ \phi^{-1}_{h,A(h)}(y) \tag{7}$$

are identical, and when $y = 1$ this specializes to

$$\phi^{-1}_{h,A(h)}(x) = z_x. \tag{8}$$

Note that Equations (7) and (8) hold for every $x \in G$. Thus,

$$\Phi_h(x \circ y) = \phi^{-1}_{h,A(h)}(x \circ y) \overset{(7)}{=} z_x \circ \phi^{-1}_{h,A(h)}(y) \overset{(8)}{=} \phi^{-1}_{h,A(h)}(x) \circ \phi^{-1}_{h,A(h)}(y) = \Phi_h(x) \circ \Phi_h(y)\,, \quad x, y \in G\,.$$

Explanation A.6. A permutation $\rho\colon G \to G$ on a group G that fixes the identity is called an *orthomorphism* if $g \mapsto g^{-1} \circ \rho(g)$ is also a permutation. If ρ is an automorphism, then equivalently $g \mapsto \rho(g) \circ g^{-1}$ is a permutation.

Note that Φ_h is a permutation by definition and that we have shown that $H \cong \Phi(H) \leqslant \mathsf{Aut}(G)$. If Φ_h is an orthomorphism it implies that it is a fixed-point free automorphism: $g = \Phi_h(g) \Rightarrow g^{-1} \circ \Phi_h(g) = 1 = 1^{-1} \circ \Phi_h(1)$, and since $g \mapsto g^{-1} \circ \Phi_h(g)$ is a permutation, it implies that $g = 1$. Thus, proving that Φ_h is an orthomorphism shows that $\Phi(H)$ is a group of fixed-point free automorphisms, completing the proof of Theorem 3.1.

František Matúš, Institute of Information Theory and Automation, The Czech Academy of Sciences, Pod Vodárenskou věží 4, 182 08 Praha 8. Czech Republic.

Aner Ben-Efraim, Computer Science Dept., Ariel University, Ariel. Israel.
e-mail: anermosh@post.bgu.ac.il