Forum of Mathematics, Sigma (2024), **Vol. 12**:e104 1–16
doi:10.1017/fms.2024.121

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

A complete classification of shuffle groups

Binzhou Xia[1], Junyang Zhang[2], Zhishuo Zhang[3] and Wenying Zhu[4]

[1]School of Mathematics and Statistics, The University of Melbourne, Parkville, VIC, 3010, Australia;
E-mail: binzhoux@unimelb.edu.au.
[2]School of Mathematical Sciences, Chongqing Normal University, Chongqing, 401331, P. R. China;
E-mail: jyzhang@cqnu.edu.cn.
[3]School of Mathematics and Statistics, The University of Melbourne, Parkville, VIC, 3010, Australia;
E-mail: zhishuoz@student.unimelb.edu.au (corresponding author).
[4]School of Mathematical Sciences, and Hebei Center for Applied Mathematics, Hebei Normal University, Shijiazhuang, 050024, P. R. China; E-mail: zfwenying@mail.bnu.edu.cn.

Received: 23 October 2023; **Revised:** 24 September 2024; **Accepted:** 11 October 2024

2020 Mathematical Subject Classification: *Primary* – 20B35

Abstract

For positive integers k and n, the shuffle group $G_{k,kn}$ is generated by the $k!$ permutations of a deck of kn cards performed by cutting the deck into k piles with n cards in each pile, and then perfectly interleaving these cards following a certain permutation of the k piles. For $k = 2$, the shuffle group $G_{2,2n}$ was determined by Diaconis, Graham and Kantor in 1983. The Shuffle Group Conjecture states that, for general k, the shuffle group $G_{k,kn}$ contains A_{kn} whenever $k \notin \{2, 4\}$ and n is not a power of k. In particular, the conjecture in the case $k = 3$ was posed by Medvedoff and Morrison in 1987. The only values of k for which the Shuffle Group Conjecture has been confirmed so far are powers of 2, due to recent work of Amarra, Morgan and Praeger based on Classification of Finite Simple Groups. In this paper, we confirm the Shuffle Group Conjecture for all cases using results on 2-transitive groups and elements of large fixed point ratio in primitive groups.

1. Introduction

For a deck of $2n$ cards, the usual way to perfectly shuffle the deck is to first cut the deck in half (see Figure 1) and then perfectly interleave the two halves. There are two kinds of such shuffles according to whether the original top card remains on top or not (see Figures 2 and 3). Note that these two shuffles are permutations of the $2n$ cards. To exactly know what permutations of the cards can be achieved by performing a sequence of these two shuffles, one needs to determine the permutation group generated by these two shuffles. In 1983, Diaconis, Graham and Kantor [8] completely determined this group for all n (see Theorem 1.1). Moreover, at the end of [8], they suggested a more general problem: For an integer $k \geq 2$, if a deck of kn cards are divided into k piles with n cards in each pile, then there are $k!$ possible orders of picking up the piles to perfectly interleave. Therefore, there are $k!$ such ways to perfectly shuffle the kn cards, and one may consider the group generated by these $k!$ permutations.

Throughout this paper, for a positive integer m, we set

$$[m] = \{0, 1, \ldots, m-1\}.$$

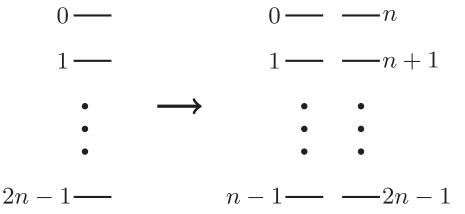

Figure 1. *Cut the deck.*

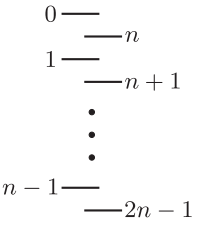

Figure 2. *Out-shuffle.*

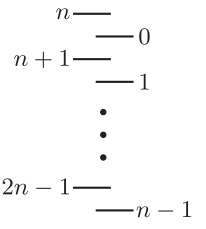

Figure 3. *In-shuffle.*

For a deck of kn cards, the card in position $i+jn$, where $i \in [n]$ and $j \in [k]$, refers to the $(i+jn)$-th card from top to bottom with the top one being the 0-th card. We may also think of them in k piles such that the j-th pile consists of the cards in the positions $jn, 1+jn, \ldots, n-1+jn$, where $j \in \{0, 1, \ldots, k-1\}$. The *standard shuffle* of the kn cards, denoted by σ, is performed by picking up the top card from each of the piles $0, \ldots, k-1$ in order and repeating until all cards have been picked up; that is, σ is the permutation of $[kn]$ defined by

$$(i+jn)^{\sigma} = ik + j \ \text{ for all } \ i \in [n] \ \text{ and } \ j \in [k].$$

Let $\tau \in \mathrm{Sym}([k])$ be a permutation of the k piles. Then τ induces a permutation ρ_τ of the kn cards by keeping the order of the cards within each pile, so that

$$(i+jn)^{\rho_\tau} = i + j^{\tau}n \ \text{ for all } \ i \in [n] \ \text{ and } \ j \in [k]. \tag{1}$$

The card shuffle $\rho_\tau\sigma$ is to first perform ρ_τ and then σ; that is,

$$(i+jn)^{\rho_\tau\sigma} = (i+j^{\tau}n)^{\sigma} = ik + j^{\tau} \ \text{ for all } \ i \in [n] \ \text{ and } \ j \in [k].$$

The subgroup of $\mathrm{Sym}([kn])$ generated by $\rho_\tau\sigma$ for all $\tau \in \mathrm{Sym}([k])$ is called the *shuffle group* on kn cards and denoted by $G_{k,kn}$; that is,

$$G_{k,kn} = \langle \rho_\tau\sigma \mid \tau \in \mathrm{Sym}([k]) \rangle = \langle \sigma, \rho_\tau \mid \tau \in \mathrm{Sym}([k]) \rangle.$$

In this terminology, what is suggested at the end of [8] is to determine the shuffle group $G_{k,kn}$.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

For a positive integer m, let C_m, A_m and S_m be the cyclic group of order m, alternating group on m points and symmetric group on m points, respectively. In 1983, Diaconis, Graham and Kantor [8] completely determined $G_{2,2n}$ as follows.

Theorem 1.1 (Diaconis-Graham-Kantor). *For $G = G_{2,2n}$, the following hold:*

(a) *If $n \equiv 0 \pmod 4$, $n > 12$ and n is not a power of 2, then $G = C_2^{n-1} \rtimes A_n$.*
(b) *If $n \equiv 1 \pmod 4$, then $G = C_2^n \rtimes A_n$.*
(c) *If $n \equiv 2 \pmod 4$ and $n > 6$, then G is the imprimitive wreath product $C_2 \wr S_n$.*
(d) *If $n \equiv 3 \pmod 4$, then $G = C_2^{n-1} \rtimes S_n$ is the Weyl group of the root system D_n.*
(e) *If $n = 2^m$ for some positive integer m, then G is the primitive wreath product $C_2 \wr C_{m+1}$.*
(f) *If $n = 6$, then $G = C_2^6 \rtimes \mathrm{PGL}(2,5)$.*
(g) *If $n = 12$, then $G = C_2^{11} \rtimes M_{12}$, where M_{12} is the Mathieu group on 12 points.*

In 1987, Medvedoff and Morrison [13] initiated a systematic study of the shuffle group $G_{k,kn}$ for general k. They showed (see [13, Theorem 2]) that, if n is a power of k, then $G_{k,kn}$ is the primitive wreath product of S_k by the cyclic group of order $\log_k(kn)$; that is,

$$G_{k,k^m} = S_k \wr C_m. \tag{2}$$

Moreover, based on computation results, Medvedoff and Morrison conjectured in [13] that $G_{3,3n}$ contains A_{3n} if n is not a power of 3, which is essentially a conjectural classification of $G_{3,3n}$ (see the Remark after Conjecture 1.2). Similarly, they made a conjecture for $k = 4$ in the same paper, which states that $G_{4,4n}$ contains A_{4n} if n is not a power of 2, and $G_{4,4n}$ is the full affine group of degree $4n$ if n is an odd power of 2. The latter part of this conjecture, that is,

$$G_{4,2^{2\ell+1}} = \mathrm{AGL}(2\ell+1, 2), \tag{3}$$

was confirmed in 2005 by Cohen, Harmse, Morrison and Wright [7, Theorem 2.6]. This leads them to the following conjecture.

Conjecture 1.2 (Shuffle Group Conjecture). *For $k \geq 3$, if n is not a power of k and $(k,n) \neq (4, 2^f)$ for any positive integer f, then $G_{k,kn}$ contains A_{kn}.*

Remark. From the definitions of σ and ρ_τ, it is not hard to see that $G_{k,kn}$ is a subgroup of A_{kn} if and only if either $n \equiv 2 \pmod 4$ and $k \equiv 0$ or $1 \pmod 4$, or $n \equiv 0 \pmod 4$ (see, for example, [13, Theorem 1]). This implies that $G_{k,kn}$ is precisely determined if we know that $G_{k,kn}$ contains A_{kn}. Therefore, the above Shuffle Group Conjecture is in fact a conjectural classification of the shuffle groups $G_{k,kn}$ for all $k \geq 3$ and $n \geq 1$.

Among other results, Amarra, Morgan and Praeger [1] recently confirmed Conjecture 1.2 for the following three cases:

(i) $k > n$;
(ii) k and n are powers of the same integer $\ell \geq 2$;
(iii) k is a power of 2, and n is not a power of 2.

Note that (ii) and (iii) together imply the validity of Conjecture 1.2 whenever k is a power of 2. We also remark that the Classification of Finite Simple Groups (CFSG) comes into play in the study of shuffle groups in [1]. In fact, CFSG was already applied in an unpublished result of William Kantor (see [11] and [13, Page 13]) to prove that $G_{k,kn} \geq A_{kn}$ if $k \geq 4$ and k does not divide n.

In this paper, we prove Conjecture 1.2 for all k and n (see Theorems 1.3 and 1.4). Our approach is to reduce the proof of the conjecture to that of the 2-transitivity of $G_{k,kn}$ by considering the fixed point ratio of certain element therein. This approach makes use of some deep classification results (depending on CFSG) in group theory – for example, the classification of 2-transitive groups and primitive groups with elements of large fixed point ratio [4, 10, 12]. Our reduction theorem is as follows.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Theorem 1.3. *If $G_{k,kn}$ is 2-transitive with $k \geq 3$, then either $k = 4$ and n is an odd power of 2, or $G_{k,kn}$ contains A_{kn}.*

By Theorem 1.3, we can determine $G_{k,kn}$ for $k \geq 3$ if it is shown to be 2-transitive. This is the case when n is not a power of k, as the following theorem states.

Theorem 1.4. *The shuffle group $G_{k,kn}$ is 2-transitive if $k \geq 3$ and n is not a power of k.*

The combination of Theorems 1.3 and 1.4 completely solves Conjecture 1.2 affirmatively. Now that Conjecture 1.2 is confirmed, it together with [13, Theorem 2] and [7, Theorem 2.6] leads to (see the remark after Conjecture 1.2) the following complete classification of shuffle groups.

Theorem 1.5. *If $k \geq 3$, then the following hold:*

(a) *If $kn = k^m$, then $G_{k,kn}$ is the primitive wreath product $S_k \wr C_m$.*
(b) *If $k = 4$ and $kn = 2^m$ with m odd, then $G_{k,kn}$ is the affine group* $\mathrm{AGL}(m, 2)$.
(c) *If n is not a power of k and either n is odd or both $n/2$ and $k(k-1)/2$ are odd integers, then $G_{k,kn} = S_{kn}$.*
(d) *In all other cases, $G_{k,kn} = A_{kn}$.*

The remainder of this paper is structured as follows. In the next section, we will give definitions and some technical lemmas that will be used in Section 3. After this preparation, Theorem 1.3 will be proved in Section 3, and the proof of Theorems 1.4 will be given in Section 4. Finally, in Section 5, we conclude the paper with some open problems on the so-called generalised shuffle groups introduced by Amarra, Morgan and Praeger [1].

2. Preliminaries

For a finite group G, let $\mathbf{Z}(G)$ denote the centre of G, let $\mathbf{O}_p(G)$ denote the largest normal p-subgroup of G for a prime p, and let $\mathbf{C}_G(g)$ denote the centraliser of an element g in G. The *socle* of G is the product of the minimal normal subgroups of G, denoted by $\mathrm{Soc}(G)$. The *fixed point ratio* of a permutation g on a finite set Ω, denoted by $\mathrm{fpr}(g)$, is defined by

$$\mathrm{fpr}(g) = \frac{|\mathrm{Fix}(g)|}{|\Omega|},$$

where $\mathrm{Fix}(g) = \{\alpha \in \Omega \mid \alpha^g = \alpha\}$.

Lemma 2.1. *Let g be an element of* $\mathrm{PGL}(d, 3)$ *acting on the set of 1-dimensional subspaces of the vector space $\mathbb{F}_3^d$. Then*

$$\mathrm{fpr}(g) = \frac{3^s + 3^t - 2}{3^d - 1}$$

for some nonnegative integers s and t.

Proof. Let $\hat{g} \in \mathrm{GL}(d, 3)$ such that $g = \hat{g}\mathbf{Z}(\mathrm{GL}(d, 3)) \in \mathrm{PGL}(d, 3)$. Note that a 1-dimensional subspace $\langle v \rangle$ of $\mathbb{F}_3^d$ satisfies $\langle v \rangle^g = \langle v \rangle$ if and only if $v^{\hat{g}}$ is v or $-v$. Therefore,

$$\mathrm{Fix}(g) = \{\langle v \rangle \mid v \in \mathbb{F}_3^d \setminus \{0\},\ v^{\hat{g}} = v\} \cup \{\langle v \rangle \mid v \in \mathbb{F}_3^d \setminus \{0\},\ v^{\hat{g}} = -v\},$$

and hence,

$$\mathrm{fpr}(g) = \frac{|\mathrm{Fix}(g)|}{|\{\langle v \rangle \mid v \in \mathbb{F}_3^d \setminus \{0\}\}|} = \frac{\frac{3^s-1}{2} + \frac{3^t-1}{2}}{\frac{3^d-1}{2}} = \frac{3^s + 3^t - 2}{3^d - 1},$$

where s and t are the dimensions of the 1-eigenspace and (-1)-eigenspace of $\hat{g}$, respectively. □

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Let $V = \mathbb{F}_q^d$ be a d-dimensional vector space over $\mathbb{F}_q$, where $d \geq 3$ and q is even, and we fix an ordered basis of V and associate each element of $\mathrm{SL}(V)$ with its matrix under this basis. For an involution $g \in \mathrm{SL}(V)$, denote by $r(g)$ the number of Jordan blocks of size 2 in the Jordan canonical form of g. Note that two involutions A and B in $\mathrm{SL}(V)$ are conjugate in $\mathrm{SL}(V)$ if and only if $r(A) = r(B)$. For an integer ℓ with $1 \leq \ell \leq d/2$, denote

$$A_\ell = \begin{pmatrix} I_\ell & & \\ & I_{d-2\ell} & \\ I_\ell & & I_\ell \end{pmatrix},$$

where I_j is the $j \times j$ identity matrix. It is clear that A_ℓ is an involution in $\mathrm{SL}(V)$ with $r(A_\ell) = \ell$. We call A_ℓ the *Suzuki form* of the conjugacy class of A_ℓ in $\mathrm{SL}(V)$.

For $\varepsilon \in \{+, -\}$, let $\mathrm{O}^\varepsilon(2m, q)$ be the general orthogonal group of ε type on the space $\mathbb{F}_q^{2m}$, where m is a positive integer and q is a prime power. For convenience, we set the notation $\mathrm{Sp}(0, q)$ and $\mathrm{O}^\varepsilon(0, q)$ to be the trivial group. The following lemma is a consequence of [2, Sections 7 and 8].

Lemma 2.2. *For each involution $g \in \mathrm{O}^\varepsilon(2m, 2) < \mathrm{Sp}(2m, 2)$, we have*

$$\frac{|\mathbf{C}_{\mathrm{Sp}(2m,2)}(g)|}{|\mathbf{C}_{\mathrm{O}^\varepsilon(2m,2)}(g)|} = \frac{|\mathrm{Sp}(2m-2r,2)| \cdot |\mathbf{O}_2(\mathbf{C}_{\mathrm{Sp}(2m,2)}(g))|}{|\mathrm{O}^\varepsilon(2m-2r,2)| \cdot |\mathbf{O}_2(\mathbf{C}_{\mathrm{O}^\varepsilon(2m,2)}(g))|}$$

for some positive integer $r \leq m$.

Proof. Write $G = \mathrm{Sp}(2m, 2)$ and $H = \mathrm{O}^\varepsilon(2m, 2)$. Since $g \in G$, we see that there exists a basis of $\mathbb{F}_2^{2m}$ as in (1), (2) or (3) of [2, (7.6)] such that g is in Suzuki form under this basis. For convenience, we say that g has form a_ℓ, b_ℓ or c_ℓ, if the basis is chosen as in (1), (2) or (3) of [2, (7.6)], respectively.

First assume that g has form a_ℓ (in this case, ℓ is even). It follows from [2, (7.9)] that there exists a homomorphism from $\mathbf{C}_G(g)$ onto $\mathrm{Sp}(\ell, 2) \times \mathrm{Sp}(2m - 2\ell, 2)$ with kernel $\mathbf{O}_2(\mathbf{C}_G(g))$. Therefore,

$$\frac{|\mathbf{C}_G(g)|}{|\mathbf{O}_2(\mathbf{C}_G(g))|} = |\mathrm{Sp}(\ell, 2) \times \mathrm{Sp}(2m - 2\ell, 2)|.$$

Moreover, [2, (8.6)] shows that there is a homomorphism from $\mathbf{C}_H(g)$ to $\mathrm{Sp}(\ell, 2) \times \mathrm{O}^\varepsilon(2m - 2\ell, 2)$ with kernel $\mathbf{O}_2(\mathbf{C}_H(g))$, and so

$$\frac{|\mathbf{C}_H(g)|}{|\mathbf{O}_2(\mathbf{C}_H(g))|} = |\mathrm{Sp}(\ell, 2) \times \mathrm{O}^\varepsilon(2m - 2\ell, 2)|.$$

As a consequence,

$$\frac{|\mathbf{C}_G(g)|}{|\mathbf{C}_H(g)|} = \frac{|\mathrm{Sp}(2m-2\ell,2)| \cdot |\mathbf{O}_2(\mathbf{C}_G(g))|}{|\mathrm{O}^\varepsilon(2m-2\ell,2)| \cdot |\mathbf{O}_2(\mathbf{C}_H(g))|}.$$

Now assume that g has form b_ℓ or c_ℓ (in this case, ℓ is odd or even, respectively). Similarly, we derive from [2, (7.10) and (7.11)] and [2, (8.7) and (8.8)] that

$$\frac{|\mathbf{C}_G(g)|}{|\mathbf{O}_2(\mathbf{C}_G(g))|} = |\mathrm{Sp}(\ell - 1, 2) \times \mathrm{Sp}(2m - 2\ell, 2)| = \frac{|\mathbf{C}_H(g)|}{|\mathbf{O}_2(\mathbf{C}_H(g))|}$$

or

$$\frac{|\mathbf{C}_G(g)|}{|\mathbf{O}_2(\mathbf{C}_G(g))|} = |\mathrm{Sp}(\ell - 2, 2) \times \mathrm{Sp}(2m - 2\ell, 2)| = \frac{|\mathbf{C}_H(g)|}{|\mathbf{O}_2(\mathbf{C}_H(g))|}.$$

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

It follows that

$$\frac{|\mathbf{C}_G(g)|}{|\mathbf{C}_H(g)|} = \frac{|\mathbf{O}_2(\mathbf{C}_G(g))|}{|\mathbf{O}_2(\mathbf{C}_H(g))|} = \frac{|\mathrm{Sp}(0,2)| \cdot |\mathbf{O}_2(\mathbf{C}_G(g))|}{|\mathrm{O}^\varepsilon(0,2)| \cdot |\mathbf{O}_2(\mathbf{C}_H(g))|}.$$

This completes the proof. □

3. Fixed point ratio and shuffle groups

In this section, we prove the reduction theorem (Theorem 1.3), which reduces the proof of Conjecture 1.2 to that of the 2-transitivity of $G_{k,kn}$. Recall from (1) that for $\tau \in \mathrm{Sym}([k])$, the permutation $\rho_\tau \in G_{k,kn}$ maps $i + jn$ to $i + j^\tau n$ for all $i \in [n]$ and $j \in [k]$. This leads to the following result on the fixed point ratio of ρ_τ, an observation that is the basis of our argument throughout this section.

Lemma 3.1. *For each $\tau \in \mathrm{Sym}([k])$, we have $\mathrm{fpr}(\tau) = \mathrm{fpr}(\rho_\tau)$. In particular, if τ is a transposition, then $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.*

A permutation group G on a set Ω is said to be *primitive* if the only partitions preserved by G are $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$. It is well known and easy to see that every 2-transitive group is primitive. An *affine* primitive group is a subgroup of $\mathrm{AGL}(d,p)$ that contains the socle of $\mathrm{AGL}(d,p)$, where d is a positive integer and p is prime.

Lemma 3.2. *Suppose that $G_{k,kn}$ is an affine primitive group with $k \geq 3$. Then either $k = 3$ and $n = 1$, or $k = 4$ and n is a power of 2.*

Proof. Let $G = G_{k,kn}$, and let V be a d-dimension vector space over $\mathbb{F}_p$ such that $G \leq \mathrm{AGL}(V)$, where d is a positive integer and p is prime. Then $kn = |V| = p^d$. By (1), there is a transposition $\tau \in \mathrm{Sym}([k])$ such that ρ_τ fixes the zero vector 0 in V. It follows that $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$. Since $\mathrm{Fix}(\rho_\tau) = \{v \in V \mid v^{\rho_\tau} = v\}$ is a subspace of V, we have $|\mathrm{Fix}(\rho_\tau)| = p^f$ for some nonnegative integer f. Thus, as τ is a transposition, we derive from Lemma 3.1 that

$$\frac{k-2}{k} = \mathrm{fpr}(\rho_\tau) = \frac{|\mathrm{Fix}(\rho_\tau)|}{|V|} = \frac{p^f}{p^d} = \frac{1}{p^{d-f}}.$$

Since $k \geq 3$, this implies that either $k = p = 3$, or $k = 4$ and $p = 2$. For the latter, $n = |V|/k = 2^{d-2}$ is a power of 2. Now assume that $k = p = 3$. Then $n = |V|/k = p^d/k = 3^{d-1}$, and so (2) gives $G = S_3 \wr C_d$. Since G is affine, we conclude that $d = 1$, which indicates that $n = 3^{d-1} = 1$. □

A group is said to be *almost simple* if its socle is a nonabelian simple group. It follows from the well-known Burnside's Theorem [5, §154, Theorem XIII] that 2-transitive groups are either affine or almost simple.

Proof of Theorem 1.3. Let $G = G_{k,kn}$ be 2-transitive with $k \geq 3$. If G is affine, then according to Lemma 3.2, either $k = 3$ and $n = 1$, or $k = 4$ and n is a power of 2. The former leads to $G = G_{3,3} = S_3$, which satisfies the conclusion of the theorem. For the latter, since G is 2-transitive, we conclude from (2) that n is not a power of 4, and so n is an odd power of 2, again satisfying the conclusion of the theorem. Thus, we may assume that G is almost simple for the rest of the proof.

First assume that $k \geq 4$. Take a transposition $\tau \in \mathrm{Sym}([k])$. By Lemma 3.1, we have

$$\mathrm{fpr}(\rho_\tau) = \frac{k-2}{k} \geq \frac{1}{2}.$$

Then since G is 2-transitive, it follows from [10, Theorem 1] that either $G \geq A_{kn}$, or

$$\mathrm{fpr}(\rho_\tau) = \frac{1}{2} + \frac{1}{2(2^r \pm 1)} \text{ for some } r \geq 3. \tag{4}$$

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

The former satisfies the conclusion of the theorem. Now suppose that (4) holds. It follows that

$$\mathrm{fpr}(\rho_\tau) \le \frac{1}{2} + \frac{1}{2(2^3-1)} = \frac{4}{7} < \frac{3}{5}.$$

This together with $\mathrm{fpr}(\rho_\tau) = (k-2)/k$ implies that $k < 5$. Thus, $k = 4$, which in turn yields $\mathrm{fpr}(\rho_\tau) = (k-2)/k = 1/2$, contradicting (4).

In the following, assume that $k = 3$. For convenience in the coming discussion, we first calculate $G_{3,3n}$ for $n \le 92$ by computation in Magma [3]. It turns out that, for these values of n, if n is not a power of 3, then $G_{3,3n}$ contains A_{3n}. Note by (2) that if n is a power of 3, then $G_{3,3n}$ is not 2-transitive. Thus, in the remainder of the proof, we assume $n > 92$.

Suppose for a contradiction that G does not contain A_{3n}. Since $n > 92$, it follows from the list of almost simple 2-transitive groups (see [6, Table 7.4]) that $\mathrm{Soc}(G)$ is a simple group of Lie type, say, over $\mathbb{F}_q$. In the following, we divide the proof into four cases according to $q > 4$, $q = 4$, $q = 3$ or $q = 2$. Take a transposition $\tau \in \mathrm{Sym}([3])$. We have $\mathrm{fpr}(\rho_\tau) = 1/3$ by Lemma 3.1.

Case 1: $q > 4$. In this case, $\mathrm{fpr}(\rho_\tau) = 1/3 > 4/(3q)$. Then since G is a 2-transitive group on $3n > 276$ points, it follows from [12, Theorem 1] that $\mathrm{Soc}(G) = \mathrm{PSL}(2,q)$ and $\mathrm{fpr}(\rho_\tau)$ is either $2/(q+1)$ or $(q_0+1)/(q+1)$, where $q_0 = q^{1/r}$ is a prime power for some integer $r \ge 2$. This together with $\mathrm{fpr}(\rho_\tau) = 1/3$ implies that $1/3 = 2/(q+1)$ or $1/3 \le (\sqrt{q}+1)/(q+1)$. However, this leads to $q \le 9$, and hence, $3n = q + 1 \le 10$, a contradiction.

Case 2: $q = 4$. In this case, we see from [6, Table 7.4] that G is a subgroup of either $\mathrm{P\Gamma U}(3,4)$ or $\mathrm{P\Gamma L}(d,4)$ with $d \ge 2$, which together with $n > 92$ implies that $G \le \mathrm{P\Gamma L}(d,4)$ with $d \ge 3$. Then according to [9, Proposition 3.1], the fixed point ratio of a non-identity element in G is less than

$$\min\left\{\frac{1}{2},\ \frac{1}{4} + \frac{1}{4^{d-1}}\right\} = \frac{1}{4} + \frac{1}{4^{d-1}} \le \frac{1}{4} + \frac{1}{4^2} < \frac{1}{3},$$

contradicting $\mathrm{fpr}(\rho_\tau) = 1/3$.

Case 3: $q = 3$. Recall that G is a 2-transitive group on $3n > 276$ points. Then we see from [6, Table 7.4] that G is a subgroup of $\mathrm{PGL}(d,3)$ with $d \ge 6$. It follows from Lemma 2.1 that

$$\frac{3^s + 3^t - 2}{3^d - 1} = \mathrm{fpr}(\rho_\tau) = \frac{1}{3}$$

for some nonnegative integers s and t. This yields

$$3(3^s + 3^t - 2) = 3^d - 1,$$

which is not possible.

Case 4: $q = 2$. In this case, we see from the list of almost simple 2-transitive groups that either $G = \mathrm{PSL}(d,2)$ with $d \ge 3$, or G is the group $\mathrm{Sp}(2m,2)$ for some $m \ge 3$ with point stabiliser $\mathrm{O}^{\pm}(2m,2)$.

First assume $G = \mathrm{PSL}(d,2)$ with $d \ge 3$. Then G can be viewed as $\mathrm{GL}(d,2)$ acting on the set of nonzero vectors. In this way, $\mathrm{Fix}(\rho_\tau) = \{v \in \mathbb{F}_2^d \mid v^x = v\} \setminus \{0\}$, and so $|\mathrm{Fix}(\rho_\tau)| = 2^r - 1$ for some nonnegative integer $r \le d$. It then follows from $\mathrm{fpr}(\rho_\tau) = 1/3$ that

$$\frac{1}{3} = \mathrm{fpr}(\rho_\tau) = \frac{2^r - 1}{2^d - 1}.$$

This yields

$$3 \cdot 2^r = 2^d + 2. \tag{5}$$

Since the right-hand side of (5) is congruent to 2 modulo 4, we deduce $3 \cdot 2^r \equiv 2 \pmod 4$, and thus, $r = 1$. However, this leads to $6 = 2^d + 2$, contradicting $d \ge 3$.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Now assume $G = \mathrm{Sp}(2m, 2)$ for some $m \geq 3$ with point stabiliser $\mathrm{O}^{\varepsilon}(2m, 2)$, where $\varepsilon \in \{+, -\}$. Note that ρ_τ is an involution with nonempty fixed point set. Let H be a point stabiliser of G containing ρ_τ. According to [2, (8.5)], two involutions in H are conjugate in G if and only if they are conjugate in H. Hence, $(\rho_\tau)^H = (\rho_\tau)^G \cap H$. Then by [4, Lemma 1.2(iii)], we have

$$\mathrm{fpr}(\rho_\tau) = \frac{|(\rho_\tau)^G \cap H|}{|(\rho_\tau)^G|} = \frac{|(\rho_\tau)^H|}{|(\rho_\tau)^G|} = \frac{|H| \cdot |\mathbf{C}_G(\rho_\tau)|}{|G| \cdot |\mathbf{C}_H(\rho_\tau)|} = \frac{|\mathrm{O}^{\varepsilon}(2m, 2)|}{|\mathrm{Sp}(2m, 2)|} \cdot \frac{|\mathbf{C}_G(\rho_\tau)|}{|\mathbf{C}_H(\rho_\tau)|}.$$

This in conjunction with Lemma 2.2 implies that

$$\mathrm{fpr}(\rho_\tau) = \frac{|\mathrm{O}^{\varepsilon}(2m, 2)|}{|\mathrm{Sp}(2m, 2)|} \cdot \frac{|\mathrm{Sp}(2m - 2r, 2)|}{|\mathrm{O}^{\varepsilon}(2m - 2r, 2)|} \cdot \frac{|\mathbf{O}_2(\mathbf{C}_G(\rho_\tau)|}{|\mathbf{O}_2(\mathbf{C}_H(\rho_\tau))|}$$

for some positive integer $r \leq m$. According to whether $r = m$ or $r < m$, we deduce that

$$\mathrm{fpr}(\rho_\tau) = \frac{1}{2^{m-1}(2^m + \varepsilon 1)} \cdot \frac{|\mathbf{O}_2(\mathbf{C}_G(\rho_\tau)|}{|\mathbf{O}_2(\mathbf{C}_H(\rho_\tau))|} \quad \text{or} \quad \frac{2^{m-r-1}(2^{m-r} + \varepsilon 1)}{2^{m-1}(2^m + \varepsilon 1)} \cdot \frac{|\mathbf{O}_2(\mathbf{C}_G(\rho_\tau)|}{|\mathbf{O}_2(\mathbf{C}_H(\rho_\tau))|}.$$

Since $\mathrm{fpr}(\rho_\tau) = 1/3$ and both $|\mathbf{O}_2(\mathbf{C}_G(\rho_\tau)|$ and $|\mathbf{O}_2(\mathbf{C}_H(\rho_\tau))|$ are powers of 2, it follows that

$$\frac{1}{3} = \frac{1}{2^m + \varepsilon 1} \quad \text{or} \quad \frac{2^{m-r} + \varepsilon 1}{2^m + \varepsilon 1}.$$

The former is not possible as $m \geq 3$. For the latter, we obtain

$$3 \cdot 2^{m-r} + \varepsilon 2 = 2^m \equiv 0 \pmod 4,$$

and thus, $m - r = 1$, which in turn leads to $m = 3$ and $\varepsilon = +$. However, this implies that $3n = |\mathrm{Sp}(6, 2)|/|\mathrm{O}^+(6, 2)| = 36$, contradicting $n > 92$. □

4. 2-transitivity

We will prove Theorem 1.4 in this section. Throughout this section, let $n = k^s t$ where s and t are integers satisfying $s \geq 0$, $t > 1$ and $k \nmid t$. For a nonnegative integer m and a positive integer ℓ, we use $[m]_\ell^0$ and $[m]_\ell^1$ to denote the remainder and quotient of m divided by ℓ; that is,

$$m = \ell[m]_\ell^1 + [m]_\ell^0$$

with $0 \leq [m]_\ell^0 \leq \ell - 1$. For every $x \in [kn]$ (note that $0 \leq x < k^{s+1}t$), we write $[x]_t^1$ in base k as follows: $[x]_t^1 = k^s x_s + \cdots + kx_1 + x_0$, where $x_i \in [k]$ for every $i \in [s + 1]$. Therefore, x can be uniquely written as

$$x = (k^s x_s + \cdots + kx_1 + x_0)t + [x]_t^0.$$

For convenience, we identify x with $(x_s, \ldots, x_1, x_0; X)$ where $X = [x]_t^0$, and sometimes we mix the two notations when doing addition. For example,

$$(x_s, \ldots, x_3, 0, 1, 1; t - 1) + k^2 t + 2 = (x_s, \ldots, x_3, 1, 1, 2; 1).$$

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Recall $(i+jn)^{\sigma} = ki + j$ for all $i \in [n]$ and $j \in [k]$. One can obtain inductively that

$$\begin{aligned}(x_s, \dots, x_1, x_0; X)^{\sigma^i} &= \left(\sum_{j=i}^{s} k^j x_{j-i}\right) t + k^i X + \sum_{j=0}^{i-1} k^{i-1-j} x_{s-j} \\ &= (x_{s-i}, \dots, x_1, x_0, 0, \dots, 0; 0) + k^i X + \sum_{j=0}^{i-1} k^{i-1-j} x_{s-j} \end{aligned} \tag{6}$$

for all $i \in [s+2]$ (when $i = s+1$, the tuple $(x_{s-i}, \dots, x_1, x_0, 0, \dots, 0; 0)$ in equation (6) is to be understood as 0). In particular,

$$(x_s, \dots, x_1, x_0; X)^{\sigma} = (x_{s-1}, \dots, x_0, [kX + x_s]_t^1; [kX + x_s]_t^0), \tag{7}$$

and thus,

$$(x_s, \dots, x_1, x_0; X)^{\sigma^{-1}} = ([x_0 t + X]_k^0, x_s, \dots, x_1; [x_0 t + X]_k^1). \tag{8}$$

Recalling from (1) that $(i+jn)^{\rho_\tau} = i + j^{\tau} n$, we have

$$(x_s, \dots, x_1, x_0; X)^{\rho_\tau} = (k^{s-1} x_{s-1} + \cdots + k x_1 + x_0) t + X + x_s^{\tau} n = (x_s^{\tau}, x_{s-1}, \dots, x_1, x_0; X) \tag{9}$$

for every $(x_s, \dots, x_1, x_0; X) \in [kn]$. By (6) and (9), it is clear that

$$(x_s, \dots, x_1, x_0; X)^{\sigma^i \rho_\tau \sigma^{-i}} = (x_s, \dots, x_{s-i+1}, x_{s-i}^{\tau}, x_{s-i-1}, \dots, x_1, x_0; X). \tag{10}$$

Consider the subgroup $H := \langle \sigma, \rho_\tau \mid \tau \in \mathrm{Sym}([k-1]) \rangle$ of $G_{k,kn}$, which is contained in the stabiliser of $kn - 1$. Our strategy for proving Theorem 1.4 is to prove that H is transitive on $[kn-1]$. We use $(i, j) \in \mathrm{Sym}([k])$ with $i \neq j$ to denote the transposition swapping i and j. For each $x \in [k]$, let $(0, x)$ denote the permutation of $[k]$ sending x to 0 and 0 to x while fixing $[k] \setminus \{0, x\}$ pointwise. In particular, $(0, x)$ coincides with the above notation for a transposition if $x \neq 0$ and is the identity permutation if $x = 0$. This somewhat cumbersome notation avoids discussing whether $x = 0$ in the following.

Let $x = (x_s, x_{s-1}, \dots, x_0; X) \in [kn]$. Write $\alpha_i = \sigma^i \rho_{(0,1)} \sigma^{-i}$ for every $i \in [s+1]$. By (10),

$$x^{\alpha_i} = (x_s, \dots, x_{s-i+1}, x_{s-i}^{(0,1)}, x_{s-i-1}, \dots, x_0; X).$$

Set $\beta_\tau = \sigma^{-1} \rho_\tau \sigma \in H$ for $\tau \in \mathrm{Sym}([k-1])$. Using (7)–(9), it is straightforward to check that

$$x^{\beta_\tau} = x + ([x_0 t + X]_k^0)^{\tau} - [x_0 t + X]_k^0.$$

We will use the above two formulas for α_i and β_τ repeatedly without any reference. Let

$$T(x) = |\{i \in [s+1] \mid x_i = k-1\}|.$$

Lemma 4.1. *If $T(x) = 0$, then $x \in 0^H$.*

Proof. It follows from $T(x) = 0$ that $x_i \neq k-1$ for $i \in [s+1]$. This combined with (10) shows

$$x^{\prod_{i=0}^{s} \sigma^{s-i} \rho_{(0,x_i)} \sigma^{-(s-i)}} = (x_s^{(0,x_s)}, \dots, x_0^{(0,x_0)}; X) = (0, \dots, 0; X) = X \in [t]$$

and $\prod_{i=0}^{s} \sigma^{s-i} \rho_{(0,x_i)} \sigma^{-(s-i)} \in H$. So it suffices to prove that $[t] \subseteq 0^H$. We achieve this by showing that x^H contains an integer less than x for each $x \in [t] \setminus \{0\}$.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Let $x \in [t] \setminus \{0\}$. If $[x]_k^0 = 0$, then $x^{\sigma^{-1}} = x/k < x$. If $[x]_k^0 \neq 0$ and $[x]_k^0 \neq k-1$, then $x^{\beta_\tau} = x - [x]_k^0 < x$, where $\tau = (0, [x]_k^0)$. If $[x]_k^0 = k-1$ and $[t]_k^0 \neq 1$, then $[t+x]_k^0 \notin \{0, k-1\}$, and so there exists $\tau \in \mathrm{Sym}([k-1])$ such that $([t+x]_k^0)^\tau = [t+x]_k^0 - 1$, which leads to

$$x^{\alpha_s\beta_\tau\alpha_s} = (t+x)^{\beta_\tau\alpha_s} = (t+x-1)^{\alpha_s} = x-1 < x.$$

If $[x]_k^0 = k-1$ and $[t]_k^0 = 1$, then $[t+x]_k^0 = 0$, and hence,

$$x^{\alpha_s\beta_{(0,1)}\alpha_s\sigma^{-1}} = (t+x)^{\beta_{(0,1)}\alpha_s\sigma^{-1}} = (t+x+1)^{\alpha_s\sigma^{-1}} = (x+1)^{\sigma^{-1}} = (x+1)/k < x.$$

Therefore, $[t] \subseteq 0^H$, as desired. □

Lemma 4.2. *Let $x = (x_s, x_{s-1}, \ldots, x_1, x_0; X) \in [kn-1]$. If $1 \leq T(x) \leq s$, then there exists $y = (y_s, y_{s-1}, \ldots, y_1, y_0; Y) \in x^H$ such that either $T(y) = 0$, or $y_0 = 0$, $y_1 = k-1$ and $T(x) \geq T(y)$.*

Proof. Let ℓ be the smallest integer such that $x_\ell \neq k-1$. Write

$$x^{\sigma^{-\ell}} = z = (z_s, z_{s-1}, \ldots, z_1, z_0; Z).$$

Applying (8) repeatedly, we derive $z_{s-\ell} = x_s$, $z_{s-\ell-1} = x_{s-1}, \ldots, z_1 = x_{\ell+1}$, $z_0 = x_\ell$. Since $x_0 = \cdots = x_{\ell-1} = k-1$, it follows that $T(x) \geq T(z)$. If $T(z) = 0$, then we confirm the lemma by taking $y = z$. In what follows, assume $T(z) > 0$.

Since $z_0 = x_\ell \neq k-1$ and $k \geq 3$, there exists $\tau \in \mathrm{Sym}([k-1])$ such that $|z_0^\tau - z_0| = 1$. Set

$$\mu_0 = \begin{cases} \sigma^{-1} & \text{if } [z_0 t + Z]_k^0 \neq k-1 \\ \sigma^s \rho_\tau \sigma^{-s-1} & \text{if } [z_0 t + Z]_k^0 = k-1. \end{cases}$$

Then by (8) and (10), we obtain

$$z^{\mu_0} = \begin{cases} \left([z_0 t + Z]_k^0, z_s, \ldots, z_1; [z_0 t + Z]_k^1\right) & \text{if } [z_0 t + Z]_k^0 \neq k-1 \\ \left([z_0^\tau t + Z]_k^0, z_s, \ldots, z_1; [z_0^\tau t + Z]_k^1\right) & \text{if } [z_0 t + Z]_k^0 = k-1. \end{cases}$$

If both $[z_0 t + Z]_k^0$ and $[z_0^\tau t + Z]_k^0$ are equal to $k-1$, then it follows from $|z_0^\tau - z_0| = 1$ that k divides t, a contradiction. Thus, $[z_0^\tau t + Z]_k^0 \neq k-1$ if $[z_0 t + Z]_k^0 = k-1$. Consequently, $T(z^{\mu_0}) = T(z)$.

Let j be the smallest integer such that $z_{j+1} = k-1$. Since, in particular, none of $z_1, \ldots, z_{j-1}$ is equal to $k-1$, along the same lines as the above paragraph, we can take $\mu_1, \ldots, \mu_{j-1} \in H$ such that $z^{\mu_0\mu_1\cdots\mu_{j-1}} = (w_s, w_{s-1}, \ldots, w_1, w_0; W)$ with $w_0 = z_j$, $w_1 = z_{j+1}$ and

$$T(z^{\mu_0\mu_1\cdots\mu_{j-1}}) = \cdots = T(z^{\mu_0\mu_1}) = T(z^{\mu_0}) = T(z).$$

Let $w = z^{\mu_0\mu_1\cdots\mu_{j-1}}$ and $y = w^{\sigma^s\rho_{(0,w_0)}\sigma^{-s}}$. Since $w_0 = z_j \neq k-1$ and $w_1 = z_{j+1} = k-1$, it follows from (10) that

$$y = (w_s, w_{s-1}, \ldots, w_1, w_0; W)^{\sigma^s\rho_{(0,w_0)}\sigma^{-s}} = (w_s, \ldots, w_2, k-1, 0; W)$$

and $T(y) = T(w)$. This together with $\sigma^{-\ell}\mu_0\mu_1\cdots\mu_{j-1}\sigma^s\rho_{(0,w_0)}\sigma^{-s} \in H$ and $T(x) \geq T(z) = T(w)$ completes the proof. □

Lemma 4.3. *If $T(x) = s+1$, then x^H contains an integer less than x.*

Proof. Since $x_i = k-1$ for every $i \in [s+1]$, we have

$$x = (k-1)(k^s + \cdots + k + 1)t + X = (k^{s+1} - 1)t + X = k^{s+1}t - (t - X).$$

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Observe that (6) implies

$$x^{\sigma^{s+1}} = k^{s+1}X + (k-1)\sum_{i=0}^{s} k^i = k^{s+1}(X+1) - 1.$$

Since $x = k^{s+1}t - (t - X) = kn - (t - X) < kn - 1$, it follows that $X < t - 1$, and so,

$$x - x^{\sigma^{s+1}} = k^{s+1}t - (t - X) - k^{s+1}(X+1) + 1 = (k^{s+1} - 1)(t - X - 1) > 0.$$

Thus, $x > x^{\sigma^{s+1}}$. □

Now we are ready to prove Theorem 1.4.

Proof of Theorem 1.4. Recall our notation that $n = k^s t$ with $s \geq 0$, $t > 1$ and $k \nmid t$, and H is the subgroup of $G_{k,kn}$ generated by σ and ρ_τ for all $\tau \in \mathrm{Sym}([k-1])$. Then H is contained in the stabiliser of $kn - 1$ in $G_{k,kn}$. Since $G_{k,kn}$ is transitive, it is 2-transitive if H is transitive on $[kn - 1]$. Thus, it suffices to prove that $[kn - 1] \subseteq 0^H$. Let

$$x = (x_s, x_{s-1}, \ldots, x_1, x_0; X) \in [kn - 1],$$

where $X \in [t]$ and $x_i \in [k]$ for $i \in [s+1]$. Recall that $T(x) = |\{i \in [s+1] \mid x_i = k - 1\}|$. We show $x \in 0^H$ for all $x \in [kn - 1]$ by induction on $T(x)$. The base case $T(x) = 0$ has been confirmed by Lemma 4.1. Now let $T(x) \geq 1$ and suppose that $y \in 0^H$ for all $y \in [kn - 1]$ with $T(y) < T(x)$. We will complete the proof by constructing $y \in x^H$ such that $T(y) < T(x)$.

If $T(x) = s + 1$, then since x is finite, we derive by using Lemma 4.3 repeatedly that there exists $y \in x^H$ with $T(y) < T(x)$. In the following, we assume that $1 \leq T(x) < s + 1$. By Lemma 4.2, we can further assume $x = (x_s, \ldots, x_2, k - 1, 0; X)$. The proof proceeds in two cases.

Case 1: $[t]_k^0 \neq k - 1$.

Let $z = (x_s, \ldots, x_2, k - 1, 0; Z)$, where $Z = X + 1 - [X + 1]_k^0 \equiv 0 \pmod{k}$. We first show in the next paragraph that $z \in x^H$.

If $[X]_k^0 \neq k - 1$, then letting $\tau = (0, [X]_k^0)$, we have

$$x^{\beta_\tau} = (x_s, \ldots, x_2, k - 1, 0; X - [X]_k^0) = (x_s, \ldots, x_2, k - 1, 0; X + 1 - [X + 1]_k^0) = z.$$

Now assume $[X]_k^0 = k - 1$. Then $[t + X]_k^0 \neq k - 1$ and $[t + X]_k^0 - [t]_k^0 = -1$. Letting $\tau = ([t]_k^0, [t + X]_k^0)$, we have

$$\begin{aligned} x^{\alpha_s\beta_\tau\alpha_s} &= (x_s, \ldots, x_2, k - 1, 0; X)^{\alpha_s\beta_\tau\alpha_s} \\ &= (x_s, \ldots, x_2, k - 1, 1; X)^{\beta_\tau\alpha_s} \\ &= (x_s, \ldots, x_2, k - 1, 1; X + [t]_k^0 - [t + X]_k^0)^{\alpha_s} \\ &= (x_s, \ldots, x_2, k - 1, 0; X + 1) \\ &= (x_s, \ldots, x_2, k - 1, 0; X + 1 - [X + 1]_k^0) \\ &= (x_s, \ldots, x_2, k - 1, 0; Z). \end{aligned}$$

Therefore, $z = (x_s, \ldots, x_2, k - 1, 0; Z) \in x^H$.

In view of (8), we obtain that

$$z^{\sigma^{-2}} = (0, x_s, \ldots, x_2, k - 1; Z/k)^{\sigma^{-1}} = ([(k - 1)t + Z/k]_k^0, 0, x_s, \ldots, x_2; [(k - 1)t + Z/k]_k^1)$$

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

and that, with $W := (k-1)t + (Z + t - [t]_k^0)/k$,

$$z^{\alpha_s\sigma^{-2}} = (x_s, \dots, x_2, k-1, 1; Z)^{\sigma^{-2}}$$
$$= \left([t]_k^0, x_s, \dots, x_2, k-1; \frac{Z+t-[t]_k^0}{k}\right)^{\sigma^{-1}} = \left([W]_k^0, [t]_k^0, x_s, \dots, x_2; [W]_k^1\right).$$

If $[(k-1)t + Z/k]_k^0 \neq k-1$ or $[W]_k^0 \neq k-1$, then taking $y = z^{\sigma^{-2}}$ or $y = z^{\alpha_s\sigma^{-2}}$, respectively, we have $y \in z^H = x^H$ and $T(y) = T(x) - 1 < T(x)$. This completes the proof for the case $[(k-1)t + Z/k]_k^0 \neq k-1$ or $[W]_k^0 \neq k-1$.

Next assume $[(k-1)t + Z/k]_k^0 = k-1 = [W]_k^0$, or equivalently, $t - 1 \equiv Z/k \pmod{k}$ and $(t - [t]_k^0)/k \equiv 0 \pmod{k}$. If $Z/k = 1$, then $[t]_k^0 = 2$, which together with the assumption of Case 1 implies that $k > 3$, and hence, $\beta_{(0,2)} \in H$. Thus, taking

$$\begin{aligned} y &= z^{\alpha_s\beta_{(0,2)}\alpha_s\sigma^{-2}} \\ &= (x_s, \dots, x_2, k-1, 1; k)^{\beta_{(0,2)}\alpha_s\sigma^{-2}} \\ &= (x_s, \dots, x_2, k-1, 1; k-2)^{\alpha_s\sigma^{-2}} \\ &= (x_s, \dots, x_2, k-1, 0; k-2)^{\sigma^{-2}} \\ &= (k-2, x_s, \dots, x_2, k-1; 0)^{\sigma^{-1}} \\ &= (k-2, k-2, x_s, \dots, x_2; [(k-1)t]_k^1), \end{aligned}$$

we have $y \in z^H = x^H$ and $T(y) = T(x) - 1 < T(x)$, as desired. Similarly, if $Z/k \geq 2$, then as $[t + Z]_k^0 = [t]_k^0 \notin \{0, k-1\}$, taking $\tau = ([t]_k^0, [t]_k^0 - 1)$, $\mu = (k-2, k-3)$ and

$$\begin{aligned} y &= z^{\alpha_s\beta_\tau\alpha_s\sigma^{-1}\beta_\mu\sigma\alpha_s\sigma^{-2}} \\ &= (x_s, \dots, x_2, k-1, 0; Z-1)^{\sigma^{-1}\beta_\mu\sigma\alpha_s\sigma^{-2}} \\ &= (k-1, x_s, \dots, x_2, k-1; Z/k-1)^{\beta_\mu\sigma\alpha_s\sigma^{-2}} \\ &= (k-1, x_s, \dots, x_2, k-1; Z/k-2)^{\sigma\alpha_s\sigma^{-2}} \\ &= (x_s, \dots, x_2, k-1, 1; Z-k-1)^{\sigma^{-2}} \\ &= \left([t-1]_k^0, x_s, \dots, x_2, k-1; \frac{Z+t-[t]_k^0}{k} - 1\right)^{\sigma^{-1}} \\ &= ([W-1]_k^0, [t-1]_k^0, x_s, \dots, x_2; [W-1]_k^1) \\ &= (k-2, [t-1]_k^0, x_s, \dots, x_2; [W-1]_k^1), \end{aligned}$$

we have $y \in z^H = x^H$ and $T(y) = T(x) - 1 < T(x)$, as desired. If $Z = 0$, then $[t]_k^0 = 1$, which implies that

$$z^{\alpha_s\beta_{(0,1)}} = (x_s, \dots, x_2, k-1, 1; 0)^{\beta_{(0,1)}} = (x_s, \dots, x_2, k-1, 0; t-1),$$

and then the previous two sentences show that there exists $y \in (z^{\alpha_s\beta_{(0,1)}})^H = x^H$ with $T(y) < T(x)$.

Case 2: $[t]_k^0 = k-1$.

Recall that $x = (x_s, \dots, x_2, k-1, 0; X)$. Let

$$u = (0, x_s, \dots, x_2, k-1; U) \quad \text{and} \quad v = (0, x_s, \dots, x_2, k-1; V),$$

where $U = (X - [X]_k^0)/k$ and $V = (t + X + 1 - [X]_k^0)/k$. We first show that $u, v \in x^H$.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

If $[X]_k^0 = k-1$, then $[t+X]_k^0 = k-2$, and it follows that

$$\begin{aligned} x^{\alpha_s\beta_{(k-2,k-3)}\,\alpha_s\beta_{(0,k-2)}\,\sigma^{-1}} &= (x_s,\dots,x_2,k-1,1;X)^{\beta_{(k-2,k-3)}\,\alpha_s\beta_{(0,k-2)}\,\sigma^{-1}} \\ &= (x_s,\dots,x_2,k-1,1;X-1)^{\alpha_s\beta_{(0,k-2)}\,\sigma^{-1}} \\ &= (x_s,\dots,x_2,k-1,0;X-1)^{\beta_{(0,k-2)}\,\sigma^{-1}} \\ &= (x_s,\dots,x_2,k-1,0;X-k+1)^{\sigma^{-1}} \\ &= (0,x_s,\dots,x_2,k-1;U) \\ &= u. \end{aligned}$$

If $[X]_k^0 \neq k-1$, then letting $\tau = (0,[X]_k^0)$, we have

$$x^{\beta_\tau\sigma^{-1}} = (x_s,\dots,x_2,k-1,0;X-[X]_k^0)^{\sigma^{-1}} = u.$$

Hence, it always holds that $u \in x^H$. If $[t+X]_k^0 = k-1$, then $[X]_k^0 = 0$, and thus,

$$\begin{aligned} x^{\beta_{(0,1)}\,\alpha_s\,\sigma^{-1}} &= (x_s,\dots,x_2,k-1,0;X+1)^{\alpha_s\,\sigma^{-1}} \\ &= (x_s,\dots,x_2,k-1,1;X+1)^{\sigma^{-1}} = (0,x_s,\dots,x_2,k-1;V) = v. \end{aligned}$$

If $[t+X]_k^0 \neq k-1$, then as $[t+X]_k^0 = [X]_k^0 - 1$, we obtain by taking $\tau = (0,[t+X]_k^0)$ that

$$\begin{aligned} x^{\alpha_s\beta_\tau\sigma^{-1}} &= (x_s,\dots,x_2,k-1,1;X)^{\beta_\tau\sigma^{-1}} \\ &= (x_s,\dots,x_2,k-1,1;X-[t+X]_k^0)^{\sigma^{-1}} = (0,x_s,\dots,x_2,k-1;V) = v. \end{aligned}$$

Therefore, $v \in x^H$ always holds as well.

Now we have proved $u, v \in x^H$. If $[(k-1)t+U]_k^0 \neq k-1$, then since

$$u^{\sigma^{-1}} = ([(k-1)t+U]_k^0, 0, x_s,\dots,x_2;[(k-1)t+U]_k^1),$$

it follows that $u^{\sigma^{-1}} \in x^H$ with $T(u^{\sigma^{-1}}) = T(x)-1 < T(x)$. Similarly, if $[(k-1)t+V]_k^0 \neq k-1$, then $v^{\sigma^{-1}} \in x^H$ with $T(v^{\sigma^{-1}}) = T(x)-1 < T(x)$. This completes the proof for the case $[(k-1)t+U]_k^0 \neq k-1$ or $[(k-1)t+V]_k^0 \neq k-1$.

Next assume $[(k-1)t+U]_k^0 = k-1 = [(k-1)t+V]_k^0$. Since $X-[X]_k^0 \leq X \leq t-1$,

$$\begin{aligned} u^{\sigma\,\alpha_s\,\sigma^{-1}} &= (x_s,\dots,x_2,k-1,0;X-[X]_k^0)^{\alpha_s\,\sigma^{-1}} \\ &= (x_s,\dots,x_2,k-1,1;X-[X]_k^0)^{\sigma^{-1}} = (k-1,x_s,\dots,x_2,k-1;V-1). \end{aligned}$$

Moreover, we deduce from $[(k-1)t+U]_k^0 = k-1$ that $U \geq [U]_k^0 = k-2 \geq 1$, which implies $V \geq 2$ and $0 \leq X-[X]_k^0 - k \leq t-1$. This combined with $[(k-1)t+U]_k^0 = k-1 = [(k-1)t+V]_k^0$ yields that

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

$$\begin{aligned} u^{\sigma\alpha_s\sigma^{-1}\beta_{(k-2,k-3)}\sigma\alpha_s\sigma^{-2}} &= (k-1, x_s, \ldots, x_2, k-1; V-1)^{\beta_{(k-2,k-3)}\sigma\alpha_s\sigma^{-2}} \\ &= (k-1, x_s, \ldots, x_2, k-1; V-2)^{\sigma\alpha_s\sigma^{-2}} \\ &= (x_s, \ldots, x_2, k-1, 1; X - [X]_k^0 - k)^{\alpha_s\sigma^{-2}} \\ &= (x_s, \ldots, x_2, k-1, 0; X - [X]_k^0 - k)^{\sigma^{-2}} \\ &= (0, x_s, \ldots, x_2, k-1; U-1)^{\sigma^{-1}} \\ &= (k-2, 0, x_s, \ldots, x_2; [(k-1)t + U - 1]_k^1). \end{aligned}$$

As a consequence, with $y := u^{\sigma\alpha_s\sigma^{-1}\beta_{(k-2,k-3)}\sigma\alpha_s\sigma^{-2}} \in u^H = x^H$, we finally obtain that $T(y) = T(x) - 1 < T(x)$. □

5. Open problems on generalised shuffle groups

Shuffle groups on kn cards can be considered in a more general way by restricting the permutations on the set of k piles to a subgroup of $\mathrm{Sym}([k])$. Precisely, if $P \leq \mathrm{Sym}([k])$ is a group of permutations on the set of k piles, then we define the *generalised shuffle group* on kn cards with respect to P by

$$\mathrm{Sh}(P, n) := \langle \rho_\tau\sigma \mid \tau \in P \rangle = \langle \sigma, \rho_\tau \mid \tau \in P \rangle,$$

where σ is the standard shuffle and ρ_τ is the permutation on kn cards induced by the permutation τ on the k piles. In particular, $\mathrm{Sh}(\mathrm{Sym}([k]), n)$ is exactly the group $G_{k,kn}$ studied in this paper. Generalised shuffle groups are introduced and systematically studied by Amarra, Morgan and Praeger in [1]. Among several open problems, a conjecture [1, Conjecture 1.10] made by them is that if $k \geq 3$, n is not a power of k and $(k, n) \neq (4, 2^f)$ for any positive integer f, then $\mathrm{Sh}(C_k, n)$ contains A_{kn}, where C_k is generated by the k-cycle $(0, 1, \ldots, k-1) \in \mathrm{Sym}([k])$.

Note that $\mathrm{Sh}(C_k, n) = \langle \sigma, \rho_{(0,1,\ldots,k-1)}\sigma \rangle$. Hence, the above-mentioned conjecture asserts that, somewhat surprisingly, two shuffles σ and $\rho_{(0,1,\ldots,k-1)}\sigma$ are enough to generate A_{kn} or S_{kn}. This suggests that a 'best possible' improvement to Theorem 1.5 would be the determination of $\mathrm{Sh}(C_k, n)$. It is shown in [1, Theorem 1.4(1)] that if $kn = k^m$, then

$$\mathrm{Sh}(P, n) = P \wr C_m \tag{11}$$

for any $P \leq \mathrm{Sym}([k])$. If $k = 4$ and $kn = 2^m$ with m odd, then similarly to the proof of [7, Theorem 2.6], we derive that

$$\mathrm{Sh}(C_k, n) = \mathrm{AGL}(m, 2). \tag{12}$$

According to [13, Lemma 2], the standard shuffle σ is an even permutation if and only if

$$\frac{k(k-1)}{2} \cdot \frac{n(n-1)}{2} \equiv 0 \pmod 2. \tag{13}$$

Observing that $\rho_{(0,1,\ldots,k-1)}$ is a product of n cycles of length k, we obtain that $\rho_{(0,1,\ldots,k-1)}$ is even if and only if $(k-1)n$ is even. Hence, $\mathrm{Sh}(C_k, n) \leq A_{kn}$ if and only if

$$\frac{k(k-1)}{2} \cdot \frac{n(n-1)}{2} \equiv (k-1)n \equiv 0 \pmod 2.$$

This together with (11) and (12) indicates that [1, Conjecture 1.10] is essentially the following conjectural classification of $\mathrm{Sh}(C_k, n)$ for all $k \geq 3$ and $n \geq 1$.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

Conjecture 5.1. *If $k \geq 3$ and $C_k = \langle (0, 1, \ldots, k-1) \rangle \leq \mathrm{Sym}([k])$, then the following hold:*

(a) *If $kn = k^m$, then $\mathrm{Sh}(C_k, n)$ is the primitive wreath product $C_k \wr C_m$.*
(b) *If $k = 4$ and $kn = 2^m$ with m odd, then $\mathrm{Sh}(C_k, n)$ is the affine group $\mathrm{AGL}(m, 2)$.*
(c) *If n is not a power of k and either $k(k-1)n(n-1)/4$ or $(k-1)n$ is odd, then $\mathrm{Sh}(C_k, n) = S_{kn}$.*
(d) *In all other cases, $\mathrm{Sh}(C_k, n) = A_{kn}$.*

A choice of P to make $\mathrm{Sh}(P, n)$ close to $G_{k,kn}$ is $P = A_k$. For the case $kn = k^m$, it is already known (see (11)) that $\mathrm{Sh}(A_k, n) = A_k \wr C_m$. Moreover, since ρ_τ is even for each $\tau \in A_k$, the parity of σ implies that $\mathrm{Sh}(A_k, n) \leq A_{kn}$ if and only if (13) holds. Therefore, we pose the following conjectural classification of $\mathrm{Sh}(A_k, n)$ for all $k \geq 3$ and $n \geq 1$.

Conjecture 5.2. *If $k \geq 3$, then the following hold:*

(a) *If $kn = k^m$, then $\mathrm{Sh}(A_k, n)$ is the primitive wreath product $A_k \wr C_m$.*
(b) *If $k = 4$ and $kn = 2^m$ with m odd, then $\mathrm{Sh}(A_k, n)$ is the affine group $\mathrm{AGL}(m, 2)$.*
(c) *If n is not a power of k and $k(k-1)n(n-1)/4$ is odd, then $\mathrm{Sh}(A_k, n) = S_{kn}$.*
(d) *In all other cases, $\mathrm{Sh}(A_k, n) = A_{kn}$.*

Proving this conjecture should be easier than proving Conjecture 5.1. For one reason, if k is odd, then $\mathrm{Sh}(C_k, n) \leq \mathrm{Sh}(A_k, n)$, and so the conclusion of Conjecture 5.2 is weaker in this case. For another reason, Conjecture 5.2 is closer to our Theorem 1.5 in the sense that the size of P is only reduced by half from $P = S_k$ to $P = A_k$. Thus, some ideas in the proof of Theorem 1.5 also apply to Conjecture 5.2. For example, $\rho_{(0,1,2)} \in \mathrm{Sh}(A_k, n)$ has fixed point ratio $(k-3)/k$, which is at least $1/2$ when $k \geq 6$. In this way, a parallel result to Theorem 1.3 might still be established by the approach of this paper with an ad hoc treatment for $k \in \{3, 4, 5\}$. However, we anticipate more work to be done to prove the 2-transitivity of $\mathrm{Sh}(A_k, n)$.

As a contrast to $P = C_k$ or A_k, the choice $P = \langle \mathrm{Rev}(k) \rangle$ from [13, Page 6], where $\mathrm{Rev}(k)$ is the permutation on $[k]$ sending i to $k-1-i$, will make $\mathrm{Sh}(P, n)$ never equal to $G_{k,kn}$. In fact, denoting

$$R_{k,kn} = \mathrm{Sh}(\langle \mathrm{Rev}(k) \rangle, n)$$

and $B_i = \{i, kn-1-i\}$ (can be a singleton if $i = kn-i-1$) for $i \in \{0, 1, \ldots, \lfloor (kn-1)/2 \rfloor\}$, we can verify directly that $R_{k,kn}$ preserves the set $\{B_0, B_1, \ldots, B_{\lfloor (kn-1)/2 \rfloor}\}$. If kn is even, then $\{B_0, B_1, \ldots, B_{\lfloor (kn-1)/2 \rfloor}\}$ is a block system of $R_{k,kn}$, and so $R_{k,kn} \leq C_2 \wr S_{kn/2}$ is imprimitive. If kn is odd, then $R_{k,kn}$ fixes the $((kn-1)/2)$-th card and preserves the partition $\{B_0, B_1, \ldots, B_{\lfloor (kn-1)/2 \rfloor - 1}\}$ of the rest $kn-1$ cards, which implies that $R_{k,kn}$ is intransitive with $R_{k,kn} \leq C_2 \wr S_{(kn-1)/2}$. We have the following conjecture based on computation results.

Conjecture 5.3. *Let $k \geq 2$, $n \geq 2$ and $R_{k,kn} = \mathrm{Sh}(\langle \mathrm{Rev}(k) \rangle, n)$. Suppose that kn is even and $(k, n) \neq (\ell^e, \ell^f)$ for any positive integers ℓ, e and f. Then the following hold:*

(a) *If $(k, n) = (2, 6)$ or $(6, 2)$, then $R_{k,kn} = C_2^6 \rtimes \mathrm{PGL}(2, 5)$.*
(b) *If $(k, n) = (3, 4)$, then $R_{k,kn} = A_5$.*
(c) *If $(k, n) = (4, 3)$, then $R_{k,kn} = C_2 \times A_5$.*
(d) *If $kn = 24$, then $R_{k,kn} = C_2^{11} \rtimes M_{12}$.*
(e) *If $kn \neq 12$, $k \equiv 2$ or $3 \pmod 4$ and $n \equiv 2 \pmod 4$, then $R_{k,kn} = C_2 \wr S_{kn/2}$.*
(f) *If $k \equiv 2 \pmod 4$ and $n \equiv 1 \pmod 4$, then $R_{k,kn} = C_2^{kn/2} \rtimes A_{kn/2}$.*
(g) *If $k \equiv 2 \pmod 4$ and $n \equiv 3 \pmod 4$, then $R_{k,kn} = C_2^{(kn-2)/2} \rtimes S_{kn/2}$.*
(h) *Otherwise, $R_{k,kn} = C_2^{(kn-2)/2} \rtimes A_{kn/2}$.*

Remark. Statements (a)–(d) have been verified by computation in Magma [3], and we include them in Conjecture 5.3 for completeness. In fact, statement (d) is already mentioned in [13]. The reason why we assume kn even and $(k, n) \neq (\ell^e, \ell^f)$ is that we have not yet identified the patterns of $R_{k,kn}$ if kn

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press

is odd or $(k,n) = (\ell^e, \ell^f)$ for some positive integers ℓ, e and f. However, we do have some interesting observations in special cases. For example, for $(k,n) = (\ell^e, \ell^f)$ with $\gcd(e,f) = 1$, it seems that

$$R_{k,kn} = \begin{cases} C_2^{e+f-1} \rtimes C_{e+f} & \text{if } e \equiv f+1 \equiv 0 \pmod 2 \\ C_2 \wr C_{e+f} & \text{otherwise.} \end{cases} \tag{14}$$

This would be a generalisation of [1, Theorem 1.4(1)], as the latter can be obtained from (14) by taking $e = 1$.

Finally, we would like to pose the following more challenging question.

Question 5.4. *Given $k \geq 3$ and $n \geq 1$ such that n is not a power of k and $(k,n) \neq (4, 2^f)$ for any odd integer f, for what $\theta \in \mathrm{Sym}([k])$ does $\langle \sigma, \rho_\theta \sigma \rangle = \mathrm{Sh}(\langle \theta \rangle, n)$ contain A_{kn}?*

Note that a complete answer to Question 5.4 would in particular solve Conjectures 5.1 and 5.3. Another interesting consequence would be the proportion

$$\frac{\{\theta \in \mathrm{Sym}([k]) \mid \mathrm{Sh}(\langle \theta \rangle, n) \text{ contains } A_{kn}\}}{k!}$$

of valid permutations θ in $\mathrm{Sym}([k])$ for a pair (k,n), especially when k and n are large. Our computation results suggest that this proportion is at least (for most cases much larger than) $1/6$.

Acknowledgements. The second author was supported by the Natural Science Foundation of Chongqing (CSTB2022NSCQ-MSX1054). The third author was supported by the Melbourne Research Scholarship provided by The University of Melbourne. The fourth author was supported by the China Scholarship Council (202106040068). The work was done during a visit of the fourth author to The University of Melbourne. The fourth author would like to thank The University of Melbourne for its hospitality and Beijing Normal University for consistent support. The authors wish to express their sincere gratitude to the anonymous referee for careful reading and invaluable suggestions to improve this paper.

Competing interest. The authors have no competing interest to declare.

References

[1] C. Amarra, L. Morgan and C. E. Praeger, 'Generalised shuffle groups', *Israel J. Math.* **244**(2) (2021), 807–856.
[2] M. Aschbacher and G.M. Seitz, 'Involutions in Chevalley groups over fields of even order', *Nagoya Math. J.* **63** (1976), 1–91.
[3] W. Bosma, J. Cannon and C. Playoust, 'The MAGMA algebra system I: The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.
[4] T. C. Burness, 'Simple groups, fixed point ratios and applications', in *Local Representation Theory and Simple Groups* (EMS Ser. Lect. Math.) (Eur. Math. Soc., Zürich, 2018), 267–322.
[5] W. Burnside, *Theory of Groups of Finite Order* second edn. (Cambridge University Press, Cambridge, 1911).
[6] P. J. Cameron, *Permutation Groups* (Cambridge University Press, Cambridge, 1999).
[7] A. Cohen, A. Harmse, K. E. Morrison and S. Wright, 'Perfect shuffles and affine groups', https://aimath.org/~morrison/Research/shuffles.
[8] P. Diaconis, R. L. Graham and W. M. Kantor, 'The mathematics of perfect shuffles', *Adv. Appl. Math.* **4**(2) (1983), 175–196.
[9] R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups, Special issue in honor of Helmut Wielandt', *J. Algebra* **234**(2) (2000), 743–792.
[10] R. Guralnick and K. Magaard, 'On the minimal degree of a primitive permutation group', *J. Algebra* **207**(1) (1998), 127–145.
[11] W. M. Kantor, Personal communication.
[12] M. W. Liebeck and J. Saxl, 'Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces', *Proc. Lond. Math. Soc.* (3) 63(2) (1991), 266–314.
[13] S. Medvedoff and K. Morrison, 'Groups of perfect shuffles', *Math. Mag.* **60**(1) (1987), 3–14.

https://doi.org/10.1017/fms.2024.121 Published online by Cambridge University Press