PERFECT SHUFFLES AND AFFINE GROUPS

AMANDA COHEN, ANDRÉ HARMSE, KENT E. MORRISON, AND SARAH WRIGHT

Abstract. For positive integers k and n the group of perfect k-shuffles with a deck of kn cards is a subgroup of the symmetric group S_{kn}. The structure of these groups was found for $k = 2$ by Diaconis, Graham, and Kantor and for $k \geq 3$ and a deck of k^m cards by Medvedoff and Morrison. They also conjectured that for $k = 4$ and deck size 2^m, m odd, the group is isomorphic to the group of affine transformations of an m-dimensional vector space over the field of order 2. That conjecture is proved in this paper, and a complete conjecture is stated for the the structure of the shuffle groups for all k and n.

1. Background

For positive integers k and n we consider a deck of kn cards. A **perfect shuffle** is a permutation of the deck in which the deck is split into k equal packets of n cards each and then those packets are perfectly interleaved (as if by a k-handed shuffler). There are $k!$ different perfect shuffles corresponding to the possible orderings of the k top cards of the packets. The subgroup of the symmetric group S_{kn} generated by these $k!$ permutations is denoted by $G_{k,kn}$. The classification problem for the perfect shuffle groups is to determine the algebraic structure of these permutation groups for all k and n.

In 1983 Diaconis, Graham, and Kantor [DGK] completely disposed of the two-handed shuffles, where $k = 2$ and n is arbitrary. The two-handed shuffle groups $G_{2,2n}$ exhibit **central symmetry**, which means that any pair of cards equidistant from the center of the deck end up equidistant from the center of the deck after shuffling. Numbering the cards from top to bottom as

$$1, 2, \ldots, n, n', \ldots, 2', 1',$$

the destination of card i after shuffling is determined by the destination of card i' and conversely. This symmetry means that there is an induced permutation group on the set of n centrally symmetric pairs and that $G_{2,2n}$ is a subgroup of B_n, which is the group of signed permutations. Essentially, the classification of the two-handed shuffle groups states that generically $G_{2,2n}$ is as large as possible given the parity of the generators as permutations in S_{2n} and the parity of the induced permutations in S_n. There are, however, two special cases for small deck size ($n = 6$ and 12) and one exceptional infinite family for deck sizes that are powers of 2.

For $k > 2$ the shuffle groups do not have central symmetry, and the classification of shuffle groups appears to be less complicated. We conjecture that, apart from two infinite families, all the groups are either the full symmetric groups or the alternating groups. In 1987 Medvedoff and Morrison [MM] determined the structure

Date: August 25, 2005.

1991 *Mathematics Subject Classification.* Primary 20B35; Secondary 20G40.

Key words and phrases. Permutation groups, perfect shuffles, affine groups, finite fields.

of the groups for all k and deck size kn equal to a power of k. This gives one of the infinite families. At the same time they presented computational evidence (using CAYLEY) that there was another exceptional family in which $k = 4$ and kn is an odd power of 2. Based on the results for decks of size 8 and 32 they conjectured that for m odd $G_{4,2^m}$ is isomorphic to the group of invertible affine transformations of the m-dimensional vector space over the field $\mathbf{F}_2$. The main result of this paper is a proof of that conjecture.

This leads to the question of whether more shuffle groups of the type G_{k^j,k^m} are composed of affine transformations. In Theorem 3.1 we give a complete answer to the question. The only values k, j, m for which G_{k^j,k^m} is a subgroup of the group of affine transformations are

(1) $k = 2$, $j = 1$ or 2, and $m \geq j$.
(2) $k = 3$, $j = 1$, $m \geq 1$.

The first group of this type that is not affine is $G_{9,27}$, and we show that, in fact, it is the full symmetric group S_{27}. With the new results of this paper and the previous work already mentioned, we believe that there are no more exceptional cases and that it is reasonable to conjecture the complete classification of the perfect shuffle groups. The classification for $k = 2$ is in [DGK] and summarized in [MM]. For $k \geq 3$ we have four cases. The first is proved in [MM]. The second is proved in this article. The remaining two are still unproved but there are examples and computational evidence supporting them.

Conjecture 1.1. *For $k \geq 3$ the shuffle groups $G_{k,kn}$ are the following:*

(1) *If $kn = k^m$, then $G_{k,kn}$ is isomorphic to a semi-direct product of $(S_k)^m$ with $\mathbf{Z}_m$.*
(2) *If $k = 4$ and $kn = k^m$, m odd, then $G_{k,kn}$ is isomorphic to the affine group of an m-dimensional vector space over $\mathbf{F}_2$.*
(3) *If $n \equiv 0 \pmod 4$ or if $n \equiv 2 \pmod 4$ and $k \equiv 0, 1 \pmod 4$, then $G_{k,kn}$ is the alternating group A_{kn}*
(4) *In all other cases $G_{k,kn}$ is the symmetric group S_{kn}.*

Since there is so much more in the mathematics of shuffles beyond the focus of this article, we highly recommend the book by S. Brent Morris [M]. It contains a wealth of material, including magic tricks based on shuffling, k-handed shuffles for deck sizes $kn + q$, and many other topics. It has a comprehensive bibliography of over 100 items.

2. The Main Result

In this section we show that $G_{4,2^m}$ acts on the cards as a group of affine transformations of an m-dimensional vector space over $\mathbf{F}_2$. Furthermore, when m is odd, we show that $G_{4,2^m}$ is the full affine group.

Recall that the affine group of a vector space V over a field F is the semi-direct product of the abelian group V by the group of linear automorphisms of V. The typical element (v, A) acts on V by $x \mapsto v + Ax$. Composition is given by

$$(v, A)(w, B) = (v + Aw, AB),$$

and the inverse is given by

$$(v, A)^{-1} = (-A^{-1}v, A^{-1}).$$

We denote by $\mathrm{A}_m(\mathbf{F}_q)$ the affine group of an m-dimensional vector space over $\mathbf{F}_q$. The order of this group is $q^m(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})$.

Lemma 2.1. *The affine group $\mathrm{A}_m(\mathbf{F}_2)$ is generated by*

$$(0,A),\ (0,B),\ (e_1,I), \tag{2.1}$$

where $e_1=(1,0,\cdots,0)$ and

$$A=\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0\\ 0 & 1 & 0 & 0 & \cdots & 0\\ 0 & 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 0 & 1 & & 0\\ \vdots & \vdots & \vdots & & \ddots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix},\ B=\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1\\ 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 1 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & & 0 & 0\\ \vdots & \vdots & & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Proof. From [T] we use the result that the matrices A and B generate $\mathrm{GL}_m(\mathbf{F}_2)$. Let (v,C) be any element of $\mathrm{A}_m(\mathbf{F}_2)$. Choose $D\in\mathrm{GL}_m(\mathbf{F}_2)$ such that $De_1=v$. We easily check that

$$(v,C)=(0,D)(e_1,I)(0,D^{-1})(0,C).$$

Since A and B generate $\mathrm{GL}_m(\mathbf{F}_2)$, the elements $(0,D)$, $(0,D^{-1})$, and $(0,C)$ are in the subgroup generated by $(0,A)$ and $(0,B)$. □

In the shuffle group $G_{k,kn}$ we let s_σ be the perfect shuffle associated to the permutation $\sigma\in S_k$ of the k packets. Thus, s_I is the shuffle in which the packets are not rearranged before shuffling. We use the convention that $s_\sigma s_\tau$ means that the shuffle s_σ is performed first and then the shuffle s_τ. Now define $p_\sigma := s_\sigma {s_I}^{-1}$. The effect of p_σ on the deck is to cut the cards into the k packets, rearrange the packets according to σ, and then to put the packets back together without interleaving them. Therefore, $p_\sigma p_\tau = p_{\sigma\tau}$, and this fact allows us to reduce the number of generators from the $k!$ perfect shuffles to just three: $s_I, p_{\sigma_1}, p_{\sigma_2}$, where σ_1 and σ_2 are any pair of permutations that generate S_k. Thus, we have the following lemma giving explicit generators for the four-handed shuffle groups.

Lemma 2.2. *The group $G_{4,4n}$ is generated by $s_I, p_{(1\,2)}$, and $p_{(1\,2\,3\,4)}$.*

□

Now we concentrate on the four-handed shuffles in which the deck size is 2^m. We label the cards with the elements of the vector space $\mathbf{F}_2^m$. The cards are ordered with $(0,\ldots,0)$ as the top card, followed by $(0,\ldots,0,1)$, $(0,\ldots,0,1,0)$ and so on until $(1,\ldots,1)$. Thus the cards are labeled top to bottom by the integers 0 to 2^m-1 in their binary representation. We let $e_1,e_2,\ldots,e_m$ be the standard basis of $\mathbf{F}_2^m$.

Theorem 2.3. *The group $G_{4,2^m}$ is a subgroup of $\mathrm{A}_m(\mathbf{F}_2)$.*

Proof. We need to show that each of the three generators of $G_{4,2^m}$ acts on the cards as an affine transformation. For s_I we need the following general result [MM] about $s_I\in G_{k,kn}$. Label the card positions with the integers from 0 to $kn-1$. Then s_I fixes the cards in positions 0 and $kn-1$ and for the rest it moves the card at location i to the location ki (mod $kn-1$). Now multiplication by $k=4$ and reducing modulo 2^m-1 is simply given by a cyclic shift two bits to the left on the binary representation. Therefore, s_I acts in the same way as the linear transformation with matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & & 0 \\ 0 & 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & 0 & & 0 \\ 0 & 1 & 0 & 0 & & 0 \end{pmatrix}.$$

The generator $p_{(1\,2)}$ interchanges the first and the second packets. The cards in the first packet are those with binary form $(0, 0, \ldots)$ and the cards in the second packet are those with form $(0, 1, \ldots)$. Therefore, $p_{(1\,2)}$ interchanges the vector $(0, 0, b_3, \ldots, b_m)$ with the vector $(0, 1, b_3, \ldots, b_m)$ and leaves the rest alone. This can be expressed by saying that $(b_1, b_2, \ldots, b_m)$ is mapped to $(b_1, b_1 + b_2 + 1, b_3, \ldots, b_m)$, and hence $p_{(1\,2)}$ is the affine transformation

$$\left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & & 0 \\ 1 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \end{pmatrix} \right).$$

The generator $p_{(1\,2\,3\,4)}$ cyclically permutes the packets. Cards in the same packet have the same first two bits. In the original order these first two bits are 00, 01, 10, and 11. Then $p_{(1\,2\,3\,4)}$ moves them into the order 11, 00, 01, 10. Thus, 00 is mapped to the 01 position, 01 goes to the 10 position, 10 goes to the 11 position, and 11 goes to the 00 position. This means that $p_{(1\,2\,3\,4)}$ maps $(b_1, b_2, \ldots, b_m)$ to $(b_1 + b_2, b_2 + 1, b_3, \ldots, b_m)$. Therefore, $p_{(1\,2\,3\,4)}$ is affine and has the form

$$\left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \right).$$

Each generator of the shuffle group is affine and so $G_{4,2^m}$ is a subgroup of $\mathrm{A}_m(\mathbf{F}_2)$. □

Now refer to the generators of $\mathrm{A}_m(\mathbf{F}_2)$ given in (2.1).

Lemma 2.4. *The affine transformation* $(0, A)$ *corresponds to* $p_{(2\,4)}$ *and* (e_1, I) *corresponds to* $p_{(1\,3)(2\,4)}$.

Proof. The matrix A fixes vectors beginning 00 and 10 and it switches the vectors beginning with 01 with those beginning with 11. That is exactly what $p_{(2\,4)}$ does. The affine transformation (e_1, I) changes the first bit from 0 to 1 or 1 to 0. That means that the 00 packet switches with the 10 packet, and the 01 packet switches with the 11 packet. This is the packet permutation $p_{(1\,3)(2\,4)}$. □

Lemma 2.5. *The affine transformation* $(0, B)$ *satisfies* $(0, B^2) = {s_I}^{-1}$.

Proof. In the proof of Theorem 3 we determined that s_I is the cyclic shift two places to the left, while B is the cyclic shift one place to the right. □

Theorem 2.6. *If $m = 2$ or if m is odd, then the shuffle group $G_{4,2^m}$ is the affine group $\mathrm{A}_m(\mathbf{F}_2)$. If m is even and $m \geq 4$, then $G_{4,2^m}$ is a proper subgroup of $\mathrm{A}_m(\mathbf{F}_2)$.*

Proof. With the results of the previous two lemmas, the question becomes whether the linear transformation given by B is in the shuffle group or not. For $m = 2$,

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and so corresponds to $p_{(2\,3)}$. In this case the shuffle group and the affine group are the full symmetric group S_4.

Now B has order m and so for m odd, say $m = 2j + 1$, we have

$$B^{-1} = B^{2j} = {s_I}^{-j},$$

so that B is an element of the shuffle group. Hence, the shuffle group and the affine group are the same.

Let $m = 2j$, so that $2^m = 4^j$. Then from [MM] we know that $G_{4,4^j}$ is a semi-direct product of $(S_4)^j$ with $\mathbf{Z}_j$, and so the order of the group is $j(4!)^j$. The order of $\mathrm{A}_m(\mathbf{F}_2)$ is $2^m(2^m - 1)\cdots(2^m - 2^{m-1})$, which is much larger for all $m \geq 4$. For example, $G_{4,16}$ has order 1152, while $\mathrm{A}_4(\mathbf{F}_2)$ has order 322,560. □

3. Are Any Other Shuffle Groups Affine?

When the deck size is k^m we can label the cards by the elements of $\mathbf{Z}_k^m$. Even when k is not prime, so that $\mathbf{Z}_k$ is not a field, we may consider the affine group of invertible maps on $\mathbf{Z}_k^m$ having the form $x \mapsto v + Ax$ where v is in $\mathbf{Z}_k^m$ and A is an invertible $m \times m$ matrix over the ring $\mathbf{Z}_k$. Having seen that $G_{4,2^m}$ is a subgroup of the affine group, we ask to what extent the shuffle groups G_{k^j,k^m} are subgroups of affine groups.

Theorem 3.1. *The only shuffle groups G_{k^j,k^m} that are subgroups of affine groups $\mathrm{A}_m(\mathbf{Z}_k)$ are $G_{2,2^m}$, $G_{4,2^m}$ with $m \geq 2$, and $G_{3,3^m}$. Those that are equal to the full affine group are $G_{2,2}$, $G_{4,2^m}$ with m odd, and $G_{3,3}$.*

Proof. The proof is broken into a sequence of four lemmas. □

Lemma 3.2. *The binary shuffle group $G_{2,2^m}$ is a proper subgroup of the affine group $\mathrm{A}_m(\mathbf{F}_2)$.*

Proof. The group $G_{2,2^m}$ is generated by s_I and $p_{(1\,2)}$. It is easy to check that s_I is a cyclic shift and that $p_{(1\,2)}$ is translation by e_1:

$$\begin{aligned} s_I &: (b_1, b_2, \ldots, b_m) \mapsto (b_2, b_3, \ldots, b_m, b_1) \\ p_{(1\,2)} &: (b_1, b_2, \ldots, b_m) \mapsto (1 + b_1, b_2, \ldots, b_m). \end{aligned}$$

Hence, $s_I = (0, L)$ and $p_{(1\,2)} = (e_1, I)$, where

$$L = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

One easily verifies that the group generated by these consists of the affine maps of the form (v, L^i) for $v \in \mathbf{F}_2^m$ and $i = 0, 1, 2, \ldots, m - 1$. This shows that $G_{2,2^m}$ is the semi-direct product of $\mathbf{Z}_2^m$ by $\mathbf{Z}_m$, with $\mathbf{Z}_m$ acting by a cyclic shift, as proved by Diaconis, Graham, and Kantor [DGK, Lemma 4]. In their paper s_I is the "out-shuffle" and $s_{(1\,2)} = p_{(1\,2)}s_I$ is the "in-shuffle." □

Lemma 3.3. *For $m \geq 2$ the three-handed shuffle group $G_{3,3^m}$ is a proper subgroup of the affine group $\mathrm{A}_m(\mathbf{F}_3)$ and $G_{3,3} = \mathrm{A}_1(\mathbf{F}_3)$ and is isomorphic to S_3.*

Proof. For generators of $G_{3,3^m}$ we use $s_I, p_{(1\,2)}, p_{(2\,3)}$ and check their action on the vectors $x = (x_1, \ldots, x_m)$. We find that s_I acts by mapping $(x_1, \ldots, x_m)$ to $(x_2, \ldots, x_m, x_1)$ and so it is linear with the matrix

$$L = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The generator $p_{(1\,2)}$ has the affine form (e_1, M) where M multiplies the first component by 2 and leaves the rest alone:

$$Mx = (2x_1, x_2, \ldots, x_m).$$

Finally, the generator $p_{(2\,3)}$ is the linear map M. With a little work one can determine that any affine transformation in the subgroup generated by these three elements acts on a vector x by mapping it to some cyclic permutation of $(a_1x_1 + v_1, \ldots, a_mx_m + v_m)$ where $a_i = 1, 2$ and $v_i = 0, 1, 2$. This means that each element of $G_{3,3^m}$ has the unique representation as an affine transformation (v, L^iD) for some $v \in \mathbf{F}_3^m$, $i = 0, 1, \ldots, m-1$ and D an invertible diagonal matrix. When $m = 1$ these exhaust all six of the affine transformations and give the full symmetric group on three letters. For $m \geq 2$, not all affine transformations are of this form. One may also note that the order of $G_{3,3^m}$ is $6^m m$ and the order of $\mathrm{A}_m(\mathbf{F}_3)$ is $3^m \prod_{i=0}^{m-1}(3^m - 3^i)$. When $m = 1$ these are both equal to 6, but for $m \geq 2$ the order of the affine group is larger.

In [MM] it was proved that $G_{3,3^m}$ is the semi-direct product of $(S_3)^m$ by $\mathbf{Z}_m$. The description of $G_{3,3^m}$ as affine transformations shows that this group is also the semi-direct product of the vector group $\mathbf{F}_3^m$ with the subgroup of invertible matrices $\{L^iD\}$, which is a group of order $m2^m$. □

Lemma 3.4. *For $3 \leq j \leq m$ the shuffle group $G_{2^j,2^m}$ is not a subgroup of the corresponding affine group.*

Proof. We will show that $p_{(2\,3)}$ is not in the affine group. Since $p_{(2\,3)}$ fixes the top card, which is the zero vector, if it were affine then it would be linear. The top card of the second packet is e_j, the top card of the third packet is e_{j-1}, the top card of the fourth packet is e_{j-2} and the top card of the fifth packet is $e_{j-2} + e_j$. Now, $p_{(2\,3)}$ interchanges the top cards of the second and third packets and leaves the rest alone. Therefore, $p_{(2\,3)}$ does the following:

$$\begin{aligned} e_j &\mapsto e_{j-1} \\ e_{j-1} &\mapsto e_j \\ e_{j-2} &\mapsto e_{j-2} \\ e_{j-2} + e_j &\mapsto e_{j-2} + e_j \end{aligned}$$

If $p_{(2\,3)}$ were linear then $e_{j-2}+e_j$ would map to $e_{j-2}+e_{j-1}$. Note that this argument does not work unless $j > 2$. □

Lemma 3.5. *For $k = 3$ and $2 \leq j \leq m$ or for $k \geq 4$ and $1 \leq j \leq m$, the shuffle group G_{k^j,k^m} is not a subgroup of the corresponding affine group.*

Proof. Again we consider $p_{(2\,3)}$, which must be linear in order to be affine. The top card of the second packet is e_j, the top card of the third packet is $2e_j$ Then $p_{(2\,3)}$ acts as follows:

$$\begin{aligned} e_j &\mapsto 2e_j \\ 2e_j &\mapsto e_j \end{aligned}$$

If $p_{(2\,3)}$ is linear then $4e_j = e_j$, which forces k to be 3. If $k = 3$, then the assumption that $j \geq 2$ means that there are more than k packets. The top card of packet number $k+1$ is e_{j-1} and the top card of packet $k+2$ is $e_{j-1}+e_j$. Those cards are fixed by $p_{(2\,3)}$ but if $p_{(2\,3)}$ were linear then we would have

$$p_{(2\,3)}(e_{j-1}+e_j) = p_{(2\,3)}(e_{j-1}) + p_{(2\,3)}(e_j) = e_{j-1} + 2e_j,$$

which implies that $e_j = 2e_j$ giving a contradiction. □

We have seen that with the natural labeling of the cards using $\mathbf{Z}_k^m$ the shuffle groups are generally not subgroups of the affine group. Could it be that with some other labeling of the cards, the shuffle groups are realized by affine maps? Consider the particular group $G_{9,27}$, which is the group with the smallest values of the parameters k, j, m that is not naturally affine. For this group we show that the answer is negative.

Theorem 3.6. *The group $G_{9,27}$ is the full symmetric group S_{27}.*

Proof. We are going to use a consequence of a theorem of Jordan's: a doubly transitive permutation group containing a transposition is the full symmetric group [W]. The group $G_{9,27}$, like all the shuffle groups, is transitive. In order to show that $G_{9,27}$ is doubly transitive, it is enough to show that card 2 can be moved to any location (other than 1) while the top card is fixed.

Number the cards $1, 2, \ldots, 27$. In cycle form the shuffle s_I is

$$\begin{aligned} s_I \quad = \quad & (1)(2\,10\,4)(3\,19\,7)(5\,11\,13)(6\,20\,16)(8\,12\,22) \\ & (9\,21\,25)(14)(15\,23\,17)(18\,24\,26)(27). \end{aligned}$$

We also make use of some packet switches

$$\begin{aligned} p_{(1\,2)} &= (1\,4)(2\,5)(3\,6) \\ p_{(3\,4)} &= (7\,10)(8\,11)(9\,12). \end{aligned}$$

Looking at the cards in the nine packets

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

we can see it is easy, using packet switches, to get a card in a particular position in one packet to that same position in any other packet, such as moving card 4 to any other top position, $7, 10, 13....$ So if we can move card 2 to places $4, 5$, and 6, while keeping the first card fixed, then we can easily move it to places 7 through 27. We notice that 2 and 4 are in the same three-cycle of s_I. Therefore, $2 \mapsto 4$

using $(s_I)^2$. Getting card 2 to position 5 is a little more complicated. We notice that 5 is in the same three-cycle as 11 and 13, and that 13 is also the top card in the fifth packet. So after we get card 2 to position 4, we switch packets to move it to position 13 and then shuffle once more to get to 5. So $2 \mapsto 5$ using $(s_I)^2\, p_{(2\,5)}\, s_I$. Likewise $2 \mapsto 6$ using $s_I\, p_{(4\,6)}\, s_I$. Now, keeping the top card fixed, we can get card 2 to positions 4 through 27. The only position left is 3, but $2 \mapsto 3$ using $s_I\, p_{(3,4)}\, s_I$. Therefore, the group $G_{9,27}$ is doubly transitive.

Now we look for a transposition in $G_{9,27}$. First we compute

$$\begin{aligned} p_{(1\,2)}\, s_I \quad &= \quad (1\,2\,11\,13\,5\,10\,4)(3\,20\,16\,6\,19\,7)(8\,12\,22) \\ & \qquad (9\,21\,25)(14)(15\,23\,17)(18\,24\,26)(27). \end{aligned}$$

Notice that there are disjoint cycles of orders 7, 6, and 3. If we repeat this permutation six times we get

$$(p_{(1\,2)}\, s_I)^6 = (1\,4\,10\,5\,13\,11\,2),$$

which is the inverse of the 7-cycle. The other cycles disappear because they have lengths that divide 6. Next we see that

$$p_{(1\,2)}\,(p_{(1\,2)}\, s_I)^6 = (1)(2\,10\,4)(3\,6)(5\,11\,13).$$

Raising this to the third power kills the the 3-cycles and gives the transposition

$$(p_{(1\,2)}\,(p_{(1\,2)}\, s_I)^6)^3 = (3\,6).$$

It follows that $G_{9,27}$ is S_{27}. □

4. Open Problems

Generically, the shuffle groups fall into cases (3) and (4) of Conjecture 1.1, and those cases are still open. In each worked out example, such as $G_{9,27}$, the group is shown to be doubly transitive and then a transposition or a three-cycle is found by experimentation. Unfortunately, we have not been able to prove the double transitivity in general, which is an interesting open problem by itself. Also, the discovery of a transposition or three-cycle has required computation with the cycle forms of the generators and is highly dependent on the actual values of k and n. Perhaps, some essentially different approach is required.

It seems quite possible that some infinite subfamilies could be classified. For example, with $n = 2$ and k arbitrary we have only two cards in each packet and the analysis should be much easier. For $k \equiv 0, 1 \pmod 4$ and $k \neq 4$ we expect to get the alternating group, and for $k \equiv 2, 3 \pmod 4$ we expect the symmetric group.

The shuffle groups for $k \geq 3$ are generated by three elements, but those that turn out to be symmetric or alternating groups can actually be generated by two elements. In the course of this work we also realized that the group $\mathrm{A}_3(\mathbf{F}_2) \equiv G_{4,8}$ can also be generated by just two elements. This leads us to ask which shuffle groups can be generated by two elements. A related question is that of whether all the affine groups over $\mathbf{F}_2$ (or any finite field) can be generated by two elements.

References

[DGK] P. Diaconis, R. L. Graham, W. M. Kantor. The mathematics of perfect shuffles, Adv. Appl. Math. **4** (1983) 175–196; MR 84j: 20040.

[MM] S. Medvedoff, K. E. Morrison. Groups of perfect shuffles, Math. Mag. **60** (1987) 3–14; MR 88c:20007.

[M] S. B. Morris. *Magic Tricks, Card Shuffling and Dynamic Computer Memories*, Math. Assoc. America, Washington, DC, 1998; MR 1489235.

[T] D. E. Taylor. Pairs of generators for matrix groups I, *The Cayley Bulletin* **3** (1987) 76–85; http://citeseer.ist.psu.edu/251543.html.

[W] H. Wielandt. *Finite Permutation Groups*, Translated from the German by R. Bercov, Academic Press, New York, 1964; MR 32 #1252.

Department of Mathematics, California Polytechnic State University, San Luis Obispo, CA 93407

Department of Mathematics, California Polytechnic State University, San Luis Obispo, CA 93407
Current address: Department of Mathematics, University of California at San Diego, La Jolla, CA 92093

Department of Mathematics, California Polytechnic State University, San Luis Obispo, CA 93407
E-mail address: kmorriso@calpoly.edu

Department of Mathematics, California Polytechnic State University, San Luis Obispo, CA 93407
Current address: Department of Mathematics, Dartmouth College, Hanover, NH 03755