A NOTE ON "PERFECT SHUFFLES"

RAYMOND N. FULLER

Introduction

Throughout, let n be a positive even integer. Define a **perfect shuffle on n cards** in the following way: cut the deck of n cards perfectly in half, creating two piles, which we shall refer to as the *top half* and the *bottom half*. Then interlace the two halves perfectly using a "riffle shuffle" in which the bottom card of the top half ends up on the bottom of the shuffled deck, with the bottom card of the bottom half above it, the second-to-last card of the top half above it, the second-to-last card of the bottom half above it, and so on in this manner, alternating cards from the top and bottom halves, until the entire deck is shuffled. As an example, consider a deck of ten cards labeled 1 through 10 in numerical order from the top to the bottom of our deck. The perfect shuffle results in the following ordering of the deck:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \to 6, 1, 7, 2, 8, 3, 9, 4, 10, 5.$$

Consider what happens when a perfect shuffle on n cards is iterated on the deck. One may examine the behavior of the iterations of the shuffle on decks of n cards for different positive even integers n. After experimentation, it is clear that the deck of n cards always returns to its initial ordering (why is this so?), but the number of iterations of the shuffle required to return the deck to its initial ordering varies, and depends on n. For example, on a standard deck of 52 cards, the deck returns to its initial ordering after exactly 52 iterations of the perfect shuffle. Contrast that with a deck of 32 cards, which returns to its initial ordering after exactly 10 perfect shuffles. This leads to the following definition and question:

Definition. *Define the perfect shuffle on n cards to be **maximal** if the number of iterations of the perfect shuffle on n cards required to return the deck to its initial ordering is exactly n.*

Question. *Characterize those positive even integers n for which the perfect shuffle on n cards is maximal.*

Group Theory and Number Theory

As before, let n be a positive even integer, and let $[n]$ denote the set $\{1, 2, 3, \ldots, n\}$. The perfect shuffle on n cards is a permutation $\omega \in S_n$ on $[n]$ with

$$\omega : [n] \to [n],$$

$$\omega : i \mapsto 2i \pmod{n+1} \text{ for all } i \in [n] \tag{1}$$

where S_n denotes the symmetric group on n letters. In this way, we see that the successive orderings of the cards obtained by iterating the perfect shuffle on n cards

Date: Revised 6 October 2017.

may be described as powers of ω; i.e., the position obtained by iterating the perfect shuffle k times is given by the permutation ω^k which has the property

$$\omega^k : [n] \to [n],$$

$$\omega^k : i \mapsto 2^k i \pmod{n+1} \text{ for all } i \in [n]. \tag{2}$$

Therefore, the set of all shuffles which give rise to the possible orderings of n cards via iterations of the perfect shuffle on n cards is a group, which we shall denote as G, with operation permutation multiplication (composition of function), and may be realized as the cyclic (hence abelian) subgroup of S_n generated by ω. In other words,

$$G \cong \langle \omega \rangle \lneq S_n \tag{3}$$

and so since G is cyclic it is clear that our deck of n cards will return to their original ordering after some finite number of iterations of perfect shuffles.

Let $\mathbb{Z}_m^\times$ denote the multiplicative group of units of the integers modulo m. While the isomorphism in (3) is important, the structure of G can be made even clearer via the observation in (2) that the image of an element in $[n]$ under the permutation ω^k is completely determined by the value of 2^k in $\mathbb{Z}_{n+1}^\times$. Therefore,

$$G \cong \langle \omega \rangle \cong \langle 2 \rangle \leq \mathbb{Z}_{n+1}^\times. \tag{4}$$

We observe that the order of G is a divisor of the order of $\mathbb{Z}_{n+1}^\times$ (which is a finite group), which is given by

$$\left|\mathbb{Z}_{n+1}^\times\right| = \phi(n+1) = (n+1) \prod_{p|(n+1)} \left(1 - \frac{1}{p}\right),$$

where ϕ denotes the Euler totient function, and the product above is over all primes p dividing $n+1$.

Therefore, the order of G is the order of $\langle 2 \rangle$ in $\mathbb{Z}_{n+1}^\times$; that is, the multiplicative order of $\overline{2}$ in $\mathbb{Z}_{n+1}^\times$. Or, equivalently, the smallest positive integer k such that $2^k \equiv 1 \pmod{n+1}$. We shall denote by $\text{ord}_n m$ the multiplicative order of m modulo n. The value of $\phi(n+1) = n$ if and only if $n+1$ is a prime. This gives rise to a necessary but not sufficient condition for a perfect shuffle on n cards to be maximal: $n+1$ must be a prime. The sufficient condition can be stated in terms of the following definition:

Definition. *We say thet m is a primitive root modulo n if $\overline{m}$ is a generator of $\mathbb{Z}_n^\times$. Equivalently, m is a primitive root modulo n if $\text{ord}_n m = \phi(n)$.*

We are now ready to answer the question posed in the Introduction. The perfect shuffle on n cards is maximal if and only if the order of G is equal to n. But if the order of G is n, then, by our observation (4) and the above definition, we must have $\text{ord}_2(n+1) = n = \phi(n+1)$, and conversely, and so we obtain the following theorem, the proof of which has been outlined in this note:

Theorem. *The perfect shuffle on n cards is maximal if and only if $n+1$ is a prime and 2 is a primitive root modulo $n+1$.* □

In particular, $52 + 1 = 53$ is a prime, and one can verify directly that 2 is a primitive root modulo 53, so that the perfect shuffle on 52 cards is in fact maximal. Using the theory of quadratic reciprocity (not discussed in this note), one can obtain the finer necessary condition:

Theorem. *If 2 is a primitive root modulo an odd prime p, then either $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$.* □

Of course, $53 \equiv 5 \pmod 8$.

The question of whether there exist infinitely many primes p such that 2 is a primitive root modulo p is a special case of a more general conjecture known as "Artin's Conjecture on Primitive Roots," which remains unsettled to this day.