# The Cycles of the Multiway Perfect Shuffle Permutation *

JOHN ELLIS    HONGBING FAN

*Department of Computer Science*

*University of Victoria, P.O. Box 3055*

*Victoria, British Columbia, V8W 3P6, Canada*

JEFFREY SHALLIT

*Department of Computer Science*

*University of Waterloo*

*Waterloo, Ontario, N2L 3G1, Canada*

January 30, 2002

**Abstract**

The $(k, n)$-perfect shuffle, a generalisation of the 2-way perfect shuffle, cuts a deck of $kn$ cards into $k$ equal size decks and interleaves them perfectly with the first card of the last deck at the top, the first card of the second-to-last deck as the second card, and so on. It is formally defined to be the permutation $\rho_{k,n} : i \rightarrow ki \pmod{kn+1}, i \in \{1, 2, \ldots, kn\}$. We uncover the cycle structure of the $(k, n)$-perfect shuffle permutation by a group-theoretic analysis and show how to compute representative elements from its cycles by an algorithm using $O(kn)$ time and $O((\log kn)^2)$ space. Consequently it is possible to realise the $(k, n)$-perfect shuffle via an in-place, linear-time algorithm. Algorithms that accomplish this for the 2-way shuffle have already been demonstrated.

## 1 Introduction

The $(k, n)$-*perfect shuffle* cuts a deck of $kn$ cards into $k$ equal size subdecks and interleaves those subdecks perfectly. After the shuffle, the first card of the last subdeck becomes the first card of the new deck, the first card of the second-to-last subdeck becomes the second card, and so on. See Figure 1.

This is a generalisation of the well-known *2-way perfect shuffle*. We define the $(k, n)$-*perfect shuffle permutation* to be the permutation $\rho_{k,n} : i \rightarrow ki \pmod{(kn+1)}, i \in \{1, 2, \ldots, kn\}$.

*This work was supported by the Natural Sciences and Engineering Research Council of Canada

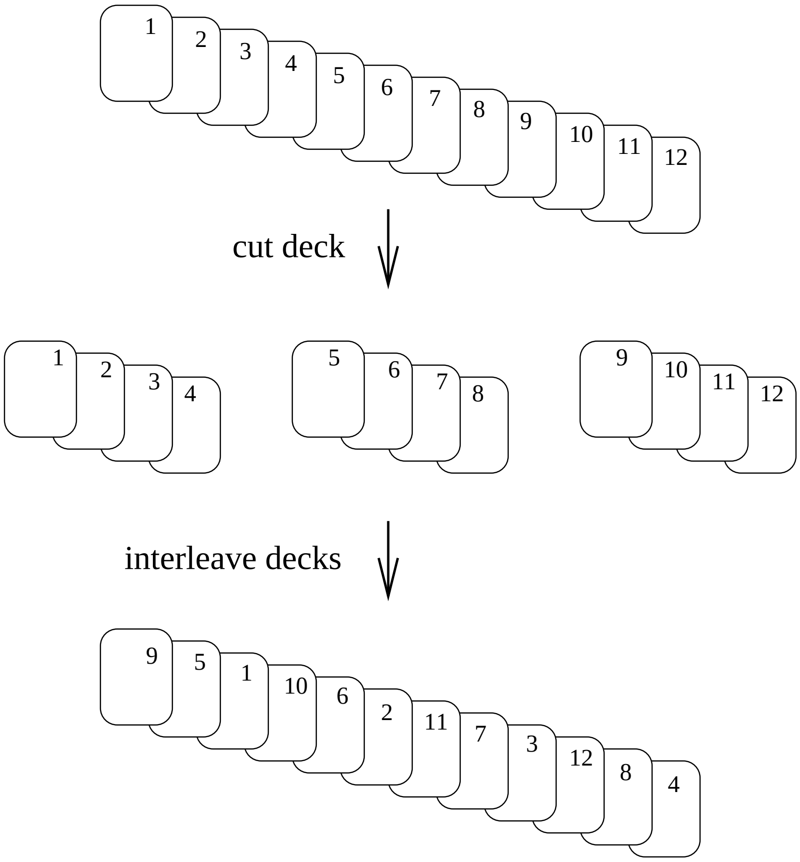


Figure 1: The $(3, 4)$-perfect shuffle illustrated

The perfect shuffle has many interesting mathematical properties and applications in computer science. The group structure of the 2-way perfect shuffle and some applications to network design are given in [DGK83] and [MM87]. A family of parallel computer architectures and associated algorithms are based on the 2-way perfect shuffle. See, for example, [Sto71, Bat91, Lei92]. In [EM00] it is shown that the classic problem of merging two lists in-place, with stability, can be reduced to the problem of accomplishing the 2-way perfect shuffle in-place. It may be that $k$-way shuffling is applicable to $k$-way merging. Hence efficient realisations of shuffling permutations could permit efficient simulation of parallel algorithms on sequential machines, and may open up new merging methods.

We have in mind the algorithmic problem of permuting, in-place, a list represented by a one-dimensional array of elements indexed by the integers 1 through $kn$. By "in-place" we mean without the use of substantial extra space over and above that which the list elements already occupy. To be precise, we allow ourselves no more than $O((\log kn)^2)$ extra bits for program variables and data structures. This definition was originally proposed by Knuth [Knu73, Section 5.5, Exercise 3]. The intention was to permit some fixed number of program variables plus recursion.

Permutations are made up of disjoint cycles and it is easy to move all the elements of one cycle, using just one extra location, by a so-called "cycle leader" algorithm [FMP95]. The method proceeds by repeatedly making a space in the list, computing the index of the element that belongs in that space and moving that element, and thus creating a new space. For example, to permute $\rho_{2,3} = (1\ 2\ 4)(3\ 6\ 5)$, we can move the elements as indicated in Figure 2. In that figure, the numbers on the arrows define the order in which the moves take place.

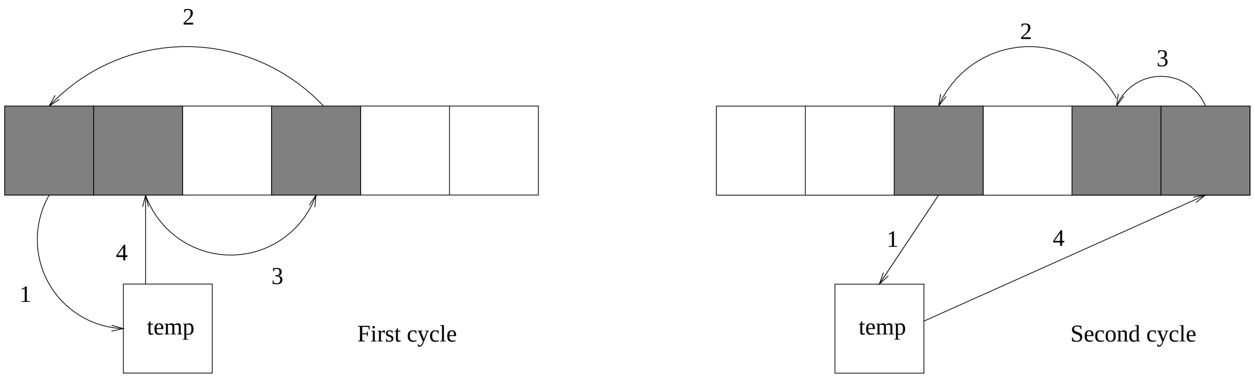


Figure 2: Realising the Perfect Shuffle

If we can easily find an unmoved element with which to start a new cycle when the current cycle terminates, then the entire task becomes easy. This is the case for some commonly used permutations such as reversal and cyclic shifts. In those cases, if the current cycle was started at location $i$ and elements remain to be moved at the end of the current cycle, then it is easy to show that the element at location $i + 1$ has yet to be moved. The problem with the perfect shuffle is that the cycle structure is more complicated, and it is no longer immediately apparent how to compute the beginning of a new cycle when needed.

We analyse the structure of the generalised perfect shuffle permutation in terms of the size, number and location of its cycles. Then we construct an in-place, $O(kn)$ time procedure that computes a set containing one element from each cycle. A cycle leader algorithm can use this set to realise the perfect shuffle in-place and in time linear in the total number of elements being shuffled.

We call this set of elements a set of *seeds* (called *cycle leaders* in [FMP95]). The seed set is a set of array indices with the following properties:

1. No two seeds are in the same cycle.

2. Every cycle contains a seed.

The methods in [FMP95] can be used to compute a seed set for any permutation of $n$ elements in time $O(n \log n)$ and using $O((\log n)^2)$ bits. We show how to compute a seed set using $O((\log kn)^2)$ space and $O(kn)$ time. A linear time and in-place algorithm for the 2-way perfect shuffle was given by Ellis and Markov [EM00]. That method does not compute a seed set. An alternative method [EKF00], which does compute a seed set, uses about half the number of moves at the expense of more arithmetic, as compared to the first method. The method described in this paper is a generalisation of this latter method. We give a characterisation of the cycles of $\rho_{k,n}$ in group theory terms and we present a linear time, in-place algorithm for computing a seed set.

## 2 The Algebraic Structure of the Cycles of $\rho_{k,n}$

We use some basic concepts from number theory and group theory. Most of them can be found in, for example, [Jon64, Agn72, Her75, BS96, **?**]. We are concerned with the ring of integers modulo $n$, where $m \pmod n$ denotes the integer that is congruent to $m$ and contained in $\{0, 1, \ldots, n-1\}$. The ring of integers modulo $n$, denoted by $\mathbb{Z}/(n)$, is the set $\{0, 1, \ldots, n-1\}$ together with operations $+$ and $\cdot$ defined by $a + b = (a + b) \pmod n$, $a \cdot b = ab \pmod n$. Clearly, the zero element and unit element of $\mathbb{Z}/(n)$ are 0 and 1 respectively. For convenience, we write $ab$ instead of $a \cdot b$, and $x$ instead of $x \pmod n$ when $x$ is assumed to be an element of $\mathbb{Z}/(n)$. The group of units of $\mathbb{Z}/(n)$ is denoted by $(\mathbb{Z}/(n))^*$. $(\mathbb{Z}/(n))^* = \{a \in \mathbb{Z}/(n) : \gcd(a, n) = 1\}$, where gcd denotes greatest common divisor. The group $(\mathbb{Z}/(n))^*$ has $\varphi(n)$ elements, where $\varphi$ is the Euler $\varphi$ function. When $n = 2, 4, p^l$ or $2p^l$ (where $p$ is an odd prime and $l \geq 1$), there exists a primitive root of $n$, so that $(\mathbb{Z}/(n))^*$ is cyclic and $(\mathbb{Z}/(n))^*$ is isomorphic to the additive group $\mathbb{Z}/(\varphi(n))$.

Now we consider the cycle structure of the permutation $\rho_{n,k}$. Let $C$ be a cycle of $\rho_{k,n}$ and $a$ be an element of $C$. Let $m = kn + 1$. By the definition of $\rho_{k,n}$, we know that $C = (a, ka, k^2a, \ldots, k^{r-1}a)$ where $r$ is the least positive integer with $k^r a \equiv a \pmod m$. Let $g = \gcd(a, m)$ and $d = \frac{m}{g}$. Then $d \neq 1$ and $k^r \frac{a}{g} \equiv \frac{a}{g} \pmod d$ and $\gcd(k, d) = \gcd(\frac{a}{g}, d) = 1$. This implies that $k, \frac{a}{g} \in (\mathbb{Z}/(d))^*$ and that $\{1, k, \ldots, k^{r-1}\} = \langle k \rangle_d$ is a subgroup of $(\mathbb{Z}/(d))^*$ generated by $k$ and $\{\frac{a}{g}, k\frac{a}{g}, \ldots, k^{r-1}\frac{a}{g}\} = \{1, k, \ldots, k^{r-1}\}\frac{a}{g}$ is a coset of $\langle k \rangle_d$ in $(\mathbb{Z}/(d))^*$. Hence $C$ is formed from the set $\langle k \rangle_d \, \frac{a}{g}\frac{m}{d} = \{a, ka, k^2a, \ldots, k^{r-1}a\}$. That is, $C$ is formed from $\frac{m}{d}$ times a coset of $\langle k \rangle_d$ in $(\mathbb{Z}/(d))^*$.

Conversely, for any nontrivial divisor $d$ of $m$ (that is, $d|m$ and $d \neq 1$), let $\langle k \rangle_d$ be the subgroup of $(\mathbb{Z}/(d))^*$ generated by $k$, and let $r = |\langle k \rangle_d|$ and $a \in (\mathbb{Z}/(d))^*$. Then, by definition, $r$ is the least positive integer such that $k^r \equiv 1 \pmod d$ and $k^r a \equiv a \pmod d$ and $k^r \frac{am}{d} \equiv \frac{am}{d} \pmod{d\frac{m}{d}} \equiv \frac{am}{d} \pmod m$. Therefore, $(\frac{am}{d}, k\frac{am}{d}, \ldots, k^{r-1}\frac{am}{d})$ is a cycle of the $(k, n)$-perfect shuffle permutation.

In summary, we have the following theorem regarding the cycle structure of the $(n, k)$-perfect shuffle permutation:

**Theorem 1** *The $r$-tuple $(a_0, a_1, \ldots, a_{r-1})$ is a cycle of the $(k, n)$-perfect shuffle permutation if and only if there is a nontrivial divisor $d$ of $kn + 1$ and an $a \in (\mathbb{Z}/(d))^*$ such that $r$ is the least positive integer such that $k^r \equiv 1 \pmod d$ and $a_i = \frac{a(kn+1)}{d}k^i \bmod (kn + 1)$ for $i = 0, 1, \ldots, r-1$.*

**Example.** Let $k = 3$ and $n = 17$. Then $kn + 1 = 52$, and the nontrivial divisors of 52 are $2, 4, 13, 26, 52$. We then find the following cycles (not all values of $a$ are shown):

| $d$ | $a$ | cycle |
|---|---|---|
| 2 | 1 | (26) |
| 4 | 1 | (13 39) |
| 13 | 1 | (4 12 36) |
| | 2 | (8 24 20) |
| | 4 | (16 48 40) |
| | 7 | (28 32 44) |
| 26 | 1 | (2 6 18) |
| | 5 | (10 30 38) |
| | 7 | (14 42 22) |
| | 17 | (34 50 46) |
| 52 | 1 | (1 3 9 27 29 35) |
| | 5 | (5 15 45 31 41 19) |
| | 7 | (7 21 11 33 47 37) |
| | 17 | (17 51 49 43 25 23) |

# 3 The Computation of a Seed Set

In what remains we will use "divisor" to mean "nontrivial divisor". To compute a seed set it is sufficient, by Theorem 1, to compute a complete set of coset representatives of $\langle k \rangle_d$ in $(\mathbb{Z}/(d))^*$ for each divisor $d$ of $kn+1$. We can speed up this computation by using the decomposition properties of integers and abelian groups.

Let $d$ be a divisor of $kn+1$ and let the prime factorisation of $d$ be $q_1^{u_1} q_2^{u_2} \cdots q_s^{u_s}$ where $q_1 > q_2 > \cdots > q_s$. By the Chinese Remainder Theorem (see for example [BS96, Theorem 5.5.4]), we know that the mapping

$$f(x) = (f_1(x), f_2(x), \ldots, f_s(x)), \quad \text{where } f_i(x) = x \bmod q_i^{u_i} \tag{1}$$

is an isomorphism from the ring $\mathbb{Z}/(d)$ to the ring $\mathbb{Z}/(q_1^{u_1}) \oplus \mathbb{Z}/(q_2^{u_2}) \oplus \cdots \oplus \mathbb{Z}/(q_s^{u_s})$. Therefore the units of the two rings correspond to each other, so that the restriction of $f$ on $(\mathbb{Z}/(d))^*$ forms an isomorphism from the group $(\mathbb{Z}/(d))^*$ to the group

$$(\mathbb{Z}/(q_1^{u_1}) \oplus \mathbb{Z}/(q_2^{u_2}) \oplus \cdots \oplus \mathbb{Z}/(q_s^{u_s}))^* = (\mathbb{Z}/(q_1^{u_1}))^* \times (\mathbb{Z}/(q_2^{u_2}))^* \times \cdots \times (\mathbb{Z}/(q_s^{u_s}))^*$$

([BS96, Lemma 5.6.1]). Furthermore, $f$ induces an isomorphism on the group quotients,

$$f^* : (\mathbb{Z}/(d))^*/\langle k \rangle_d \to (\mathbb{Z}/(q_1^{u_1}))^* \times (\mathbb{Z}/(q_2^{u_2}))^* \times \cdots \times (\mathbb{Z}/(q_s^{u_s}))^*/\langle (f_1(k), f_2(k), \ldots, f_s(k)) \rangle$$

where $\langle (f_1(k), f_2(k), \ldots, f_s(k)) \rangle$ denotes the subgroup of $(\mathbb{Z}/(q_1^{u_1}))^* \times (\mathbb{Z}/(q_2^{u_2}))^* \times \cdots \times (\mathbb{Z}/(q_s^{u_s}))^*$ generated by $(f_1(k), f_2(k), \ldots, f_s(k))$.

If $q_i$ is an odd prime, or $q_i = 2$ and $u_i \leq 2$, then we deduce from our earlier remarks that $(\mathbb{Z}/(q_i^{u_i}))^*$ is a cyclic group. Let $g_i$ be a primitive root of $q_i^{u_i}$ and $w_i = \mathrm{ind}_{g_i} f_i(k) \pmod{q_i^{u_i}}$. Since $w_i$ is the least positive integer such that $g_i^{w_i} = f_i(k) \pmod{q_i^{u_i}}$ and $f_i(k) = k \bmod q_i^{u_i}$, $w_i$ is also the index of $k \pmod{q_i^{u_i}}$. Therefore, $(\mathbb{Z}/(q_i^{u_i}))^* = \langle g_i \rangle \cong \mathbb{Z}/(\varphi(q_i^{u_i}))$ with the isomorphism $\phi(g_i^x) = x$. Clearly, $\phi(f_i(k)) = w_i$.

If $q_i = 2$ and $u_i \geq 3$, then $i = s$. We know that $2^{u_s}$ does not have a primitive root, but the order of $5 \pmod{2^{u_s}}$ is $2^{u_s-2}$, and the set

$$\{(-1)^v 5^u : u = 0, 1, \ldots, 2^{u_s-2} - 1, v = 0, 1\}$$

forms a reduced set of residues modulo $2^{u_s}$. See for example [?], page 25. Therefore, for any odd integer $x$, there exists a unique pair $(w(x), w'(x))$ such that $w(x) \in \{0, 1, \ldots, 2^{u_s-2} - 1\}$, $w'(x) \in \{0, 1\}$ and $x \equiv (-1)^{w'(x)} 5^{w(x)} \pmod{2^{u_s}}$. Hence $(\mathbb{Z}/(2^{u_s}))^* \cong \mathbb{Z}/(2^{u_s-2}) \times \mathbb{Z}/(2)$ with isomorphism $\phi(x) = (w(x), w'(x))$. Let $w_s, w_s'$ be such that $(-1)^{w_s'} 5^{w_s} \equiv f_s(k) \equiv k \pmod{2^{u_s}}$.

Suppose that $q_s \neq 2$ or $q_s = 2$ and $u_s \leq 2$. Then the mapping

$$h((g_1^{x_2}, g_2^{x_2}, \ldots, g_s^{x_s})) = (x_1, x_2, \ldots, x_s) \tag{2}$$

is an isomorphism from the group $(\mathbb{Z}/(q_1^{u_1}))^* \times (\mathbb{Z}/(q_2^{u_2}))^* \times \cdots \times (\mathbb{Z}/(q_s^{u_s}))^*$ to the group $\mathbb{Z}/(\varphi(q_1^{u_1})) \times \mathbb{Z}/(\varphi(q_2^{u_2})) \times \cdots \times \mathbb{Z}/(\varphi(q_s^{u_s}))$ and $h$ maps $(f_1(k), f_2(k), \ldots, f_s(k)) = (g_1^{w_1}, q_2^{w_2}, \ldots, g_s^{w_s})$ to $(w_1, w_2, \ldots, w_s)$. Therefore, $h$ induces an isomorphism

$$\begin{gathered} h^* : (\mathbb{Z}/(q_1^{u_1}))^* \times (\mathbb{Z}/(q_2^{u_2}))^* \times \cdots \times (\mathbb{Z}/(q_s^{u_s}))^* / \langle (f_1(k), f_2(k), \ldots, f_s(k)) \rangle \cong \\ (\mathbb{Z}/(\varphi(q_1^{u_1})) \times \mathbb{Z}/(\varphi(q_2^{u_2})) \times \cdots \times \mathbb{Z}/(\varphi(q_s^{u_s}))) / \langle (w_1, w_2, \ldots, w_s) \rangle. \end{gathered}$$

Hence, if we take a complete set of coset representatives of $\langle (w_1, w_2, \ldots, w_s) \rangle$ in $\mathbb{Z}/(\varphi(q_1^{u_1})) \times \mathbb{Z}/(\varphi(q_2^{u_2})) \times \cdots \times \mathbb{Z}/(\varphi(q_s^{u_s}))$, transform it first by $h^{-1}$ and then by $f^{-1}$, we will obtain a set of seeds corresponding to $d$.

Alternatively, suppose that $q_s = 2$ and $u_s \geq 3$. Then $q_i, i = 1, \ldots, s-1$ are odd primes and the mapping

$$h'((g_1^{x_1}, \ldots, g_{s-1}^{x_{s-1}}, (-1)^v 5^u)) = (x_1, \ldots, x_{s-1}, u, v) \tag{3}$$

is an isomorphism from the group $(\mathbb{Z}/(p_1^{u_1}))^* \times \cdots \times (\mathbb{Z}/(p_{s-1}^{u_{s-1}}))^* \times (\mathbb{Z}/(2^{u_s}))^*$ to the group $\mathbb{Z}/(\varphi(q_1^{u_1})) \times \cdots \times \mathbb{Z}/(\varphi(q_{s-1}^{u_{s-1}})) \times \mathbb{Z}/(2^{u_s-2}) \times \mathbb{Z}/(2)$ and

$$h'((f_1(k), \ldots, f_{s-1}(k), f_s(k))) = h'((g_1^{w_1}, \ldots, g_{s-1}^{w_{s-1}}, (-1)^{w_s'} 5^{w_s})) = (w_1, \ldots, w_{s-1}, w_s, w_s').$$

Therefore, $h'$ induces an isomorphism

$$\begin{gathered} h'^* : (\mathbb{Z}/(q_1^{u_1}))^* \times \cdots \times (\mathbb{Z}/(q_{s-1}^{u_{s-1}}))^* \times (\mathbb{Z}/(2^{u_s}))^* / \langle (f_1(k), f_2(k), \ldots, f_s(k)) \rangle \cong \\ (\mathbb{Z}/(\varphi(q_1^{u_1})) \times \cdots \times \mathbb{Z}/(\varphi(q_{s-1}^{u_{s-1}})) \times \mathbb{Z}/(2^{u_s-2}) \times \mathbb{Z}/(2)) / \langle (w_1, \ldots, w_{s-1}, w_s, w_s') \rangle \end{gathered}$$

Hence, again, if we take a complete set of coset representatives of the above groups, first transform it by $h'^{-1}$ and then by $f^{-1}$, we will obtain a subset of a seed set corresponding to $d$.

The computation of the complete coset representatives of the group quotients can be accomplished using the following theorem, which is of independent interest.

**Theorem 2** *Let $s$ and $t_1, t_2, \ldots, t_s$ be positive integers and*

$$G = \mathbb{Z}/(t_1) \times \mathbb{Z}/(t_2) \times \cdots \times \mathbb{Z}/(t_s) \tag{4}$$

*be an abelian group with $(w_1, w_2, \ldots, w_s) \in G$. Let* lcm *denote the least common multiple and let $a_i, b_i, c_i$ be defined by the following relations:*

$$\begin{aligned} a_i &= \gcd(w_i, t_i), \quad 1 \le i \le s; \\ b_0 &= 1; \\ b_i &= t_i/a_i, \quad 1 \le i \le s; \\ c_i &= a_i \gcd(\mathrm{lcm}(b_0, b_1, b_2, \ldots, b_{i-1}), b_i), \quad 1 \le i \le s. \end{aligned} \tag{5}$$

*Then the following statements hold:*

(i) $|\langle(w_1, w_2, \ldots, w_s)\rangle| = \mathrm{lcm}(b_1, \ldots, b_{s-1}, b_s)$*;*

(ii) $(c_1, c_2, \ldots, c_s)$ *is the lexicographically least non-zero element and generator of the subgroup* $\langle(w_1, w_2, \ldots, w_s)\rangle$*;*

(iii) $\{(e_1, e_2, \ldots, e_s) \ : \ 0 \le e_i < c_i\}$ *is a complete set of coset representatives of* $\langle(w_1, w_2, \ldots, w_s)\rangle$ *in* $G$*.*

**Proof** We first prove (i) and (ii) by induction on $s$, the number of groups in the product (4). If $s = 1$, then $b_1 = t_1/a_1$ and $c_1 = a_1 \gcd(1, b_1) = a_1 = \gcd(w_1, t_1)$. Since $0 \le c_1 \le t_1$ and $w_1 < t_1$ and $xw_1 + yt_1 = c_1$ for some integers $x$ and $y$, it follows that $c_1 = xw_1 \bmod t_1$. Hence $c_1 \in \langle w_1 \rangle$ and $\langle c_1 \rangle \subseteq \langle w_1 \rangle$. However, $w_1 = z \gcd(w_1, t_1) = zc_1$ implies that $\langle w_1 \rangle \subseteq \langle c_1 \rangle$. Hence $\langle c_1 \rangle = \langle w_1 \rangle$. For any $t$, $1 \le t < c_1$, since $\gcd(w_1, t_1) = c_1$ and $c_1 \nmid t$, the congruence $w_1 x \equiv t \pmod{t_1}$ has no solution, so that $t \notin \langle w_1 \rangle$. Therefore $c_1$ is the lexicographically least non-zero element of $\langle w_1 \rangle$. Hence $\langle w_1 \rangle = \{xc_1 : 0 \le x < t_1/c_1\}$. It follows that $|\langle w_1 \rangle| = |\langle c_1 \rangle| = t_1/c_1 = b_1 = \mathrm{lcm}(b_1)$. Thus (i) and (ii) are true when $s = 1$.

Suppose now that (i) and (ii) are true when $1 \le s \le j-1$. We prove that they remain true for $s = j$. Clearly, the group $\langle(w_1, w_2, \ldots, w_j)\rangle$ is a subgroup of $\langle(w_1, w_2, \ldots, w_{j-1})\rangle \times \langle w_j \rangle$. By the induction hypothesis, $|\langle(w_1, w_2, \ldots, w_{j-1})\rangle| = \mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})$ and $|\langle w_j \rangle| = b_j$. Then, $\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})(w_1, w_2, \ldots, w_{j-1}) = (w_1, w_2, \ldots, w_{j-1})$ and $b_j w_j = w_j$. Since $\mathrm{lcm}(\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}), b_j) = \mathrm{lcm}(b_1, b_2, \ldots, b_j)$ and is a multiple of both $\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})$ and $b_j$, it follows that $\mathrm{lcm}(b_1, b_2, \ldots, b_j)(w_1, w_2, \ldots, w_j) = (w_1, w_2, \ldots, w_j)$. Since $\mathrm{lcm}(\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}), b_j)$ is the least common multiple of $\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})$ and $b_j$, then for any $0 \le t < \mathrm{lcm}(b_1, b_2, \ldots, b_j)$, either $0 \le t \bmod \mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}) < \mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})$ or $0 \le t \bmod b_j < b_j$. This implies that $t(w_1, w_2, \ldots, w_j) \ne (w_1, w_2, \ldots, w_j)$. Therefore, $|\langle(w_1, w_2, \ldots, w_j)\rangle| = \mathrm{lcm}(b_1, b_2, \ldots, b_j)$, and so (i) is true.

Let $(c'_1, c'_2, \ldots, c'_j)$ be the lexicographically least non-zero element in $\langle(w_1, w_2, \ldots, w_j)\rangle$. Then $(c'_1, c'_2, \ldots, c'_{j-1})$ is an element of $\langle(w_1, w_2, \ldots, w_{j-1})\rangle$. By the induction hypothesis, $(c_1, c_2, \ldots, c_{j-1})$ is the lexicographically least element of $\langle w_1, w_2, \ldots, w_{j-1} \rangle$, so that

$(c_1', c_2', \ldots, c_{j-1}') \geq (c_1, c_2, \ldots, c_{j-1})$. However, $(c_1, c_2, \ldots, c_{j-1}) \in \langle (w_1, w_2, \ldots, w_{j-1}) \rangle$. Hence there exists an integer $x$ such that $x(w_1, w_2, \ldots, w_{j-1}) = (c_1, c_2, \ldots, c_{j-1})$. But

$$x(w_1, w_2, \ldots, w_{j-1}, w_j) = (c_1, c_2, \ldots, c_{j-1}, xw_j) \geq (c_1', c_2', \ldots, c_{j-1}', c_j').$$

Hence $(c_1', c_2', \ldots, c_{j-1}') \leq (c_1, c_2, \ldots, c_{j-1})$. It follows that $(c_1', c_2', \ldots, c_{j-1}') = (c_1, c_2, \ldots, c_{j-1})$.

It remains to show that $c_j' = c_j$. Consider the mapping $f : \langle (w_1, w_2, \ldots, w_{j-1}, w_j) \rangle \to \langle w_j \rangle$ such that $f(x_1, x_2, \ldots, x_{j-1}, x_j) = x_j$. Then $f$ is a homomorphism. The kernel of $f$ is $\langle (w_1, w_2, \ldots, w_{j-1}, 0) \rangle$ and $\langle (w_1, w_2, \ldots, w_{j-1}, 0) \rangle \cong \langle (w_1, w_2, \ldots, w_{j-1}) \rangle$. Since $f$ is a homomorphism, $f(\langle (w_1, w_2, \ldots, w_{j-1}, w_j) \rangle)$ is a subgroup of $\langle w_j \rangle$ and isomorphic to the group quotient $\langle (w_1, w_2, \ldots, w_{j-1}, w_j) \rangle / \langle (w_1, w_2, \ldots, w_{j-1}, 0) \rangle$. Therefore

$$\begin{aligned}|f(\langle (w_1, w_2, \ldots, w_{j-1}, w_j) \rangle)| &= |\langle (w_1, w_2, \ldots, w_j) \rangle / \langle (w_1, w_2, \ldots, w_{j-1}, 0 \rangle| \\ &= \frac{\mathrm{lcm}(b_1, b_2, \ldots, b_j)}{\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})}.\end{aligned}$$

Since (ii) is true for a product of a single group by the initial case, $a_j$ is a lexicographically least element of $\langle w_j \rangle$ in $\mathbb{Z}/(t_j)$ and $\langle a_j \rangle = \langle w_j \rangle$. Therefore the least element of $f(\langle (w_1, w_2, \ldots, w_j) \rangle)$ in $\langle a_j \rangle$ is

$$\begin{aligned}a_j \frac{b_j}{\frac{\mathrm{lcm}(b_1, b_2, \ldots, b_j)}{\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})}} &= \frac{a_j b_j \mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})}{\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}, b_j)} \\ &= a_j \ \gcd(\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}), b_j) = c_j.\end{aligned}$$

But $c_j$ is also a generator of $f(\langle (w_1, w_2, \ldots, w_j) \rangle)$ in $\langle a_j \rangle$ and

$$|\langle c_j \rangle| = \frac{\mathrm{lcm}(b_1, b_2, \ldots, b_j)}{\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})}.$$

This implies that $c_j' = f(c_1', c_2', \ldots, c_j') \geq c_j$.

Since the image in $f$ of any element in the coset $\langle (w_1, w_2, \ldots, w_{j-1}, 0) \rangle + (0, \ldots, 0, c_j)$ is $(0, \ldots, 0, c_j)$, it follows that $(c_1, c_2, \cdots, c_{j-1}, c_j) \in \langle (w_1, w_2, \cdots, w_j) \rangle$. Then, by the choice of $(c_1', c_2', \ldots, c_j')$, $(c_1', c_2', \ldots, c_{j-1}', c_j') \leq (c_1, c_2, \ldots, c_{j-1}, c_j)$. This implies that $c_j' \leq c_j$. Therefore, $c_j' = c_j$ and $(c_1, c_2, \cdots, c_j)$ is the lexicographically least non-zero element of $\langle (w_1, w_2, \ldots, w_j) \rangle$.

By the induction hypothesis, $(c_1, c_2, \ldots, c_{j-1})$ is a generator of the group $\langle (w_1, w_2, \ldots, w_{j-1}) \rangle$ and $|\langle (c_1, c_2, \ldots, c_{j-1}) \rangle| = \mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})$. Hence we have

$$\begin{aligned}|\langle (c_1, c_2, \ldots, c_{j-1}, c_j) \rangle| &= \mathrm{lcm}(\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}), |\langle c_j \rangle|) \\ &= \mathrm{lcm}(\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1}), \frac{\mathrm{lcm}(b_1, b_2, \ldots, b_j)}{\mathrm{lcm}(b_1, b_2, \ldots, b_{j-1})}) = \mathrm{lcm}(b_1, b_2, \ldots, b_j).\end{aligned}$$

This implies that $\langle (c_1, c_2, \ldots, c_{j-1}, c_j) \rangle = \langle (w_1, w_2, \ldots, w_{j-1}, w_j) \rangle$. Hence (i) and (ii) are true.

Finally, we prove (iii). Let $E = \{(e_1, e_2, \ldots, e_s) : 0 \le e_i < c_i\}$. Let $e, e'$ be distinct elements of $E$ and, without loss of generality, assume that $e < e'$. Then $e' - e < (c_1, c_2, \ldots, c_s)$ and so $e' - e \notin \langle (w_1, w_2, \ldots, w_s) \rangle$. This implies that $e$ and $e'$ are not in the same coset of $\langle (w_1, w_2, \ldots, w_s) \rangle$ in $\mathbb{Z}/(t_1) \times \mathbb{Z}/(t_2) \times \cdots \times \mathbb{Z}/(t_s)$.

However, the number of cosets of $\langle (w_1, w_2, \ldots, w_s) \rangle$ in $\mathbb{Z}/(t_1) \times \mathbb{Z}/(t_2) \times \cdots \times \mathbb{Z}/(t_s)$ is $t_1 t_2 \cdots t_s / \mathrm{lcm}(b_1, b_2, \ldots, b_s)$, and we have

$$\begin{aligned} |E| = c_1 \cdots c_s &= a_1 \gcd(\mathrm{lcm}(b_0), b_1) \cdots a_s \gcd(\mathrm{lcm}(b_1, \ldots, b_{s-1}), b_s) \\ &= (a_1 \cdots a_s) \gcd(\mathrm{lcm}(b_0), b_1) \cdots \gcd(\mathrm{lcm}(b_1, b_2, \ldots, b_{s-1}), b_s) \\ &= \frac{(a_1 \cdots a_s)(b_1 \cdots b_s)}{\mathrm{lcm}(b_1, \ldots, b_s)} \\ &= \frac{t_1 \cdots t_s}{\mathrm{lcm}(b_1, \ldots, b_s)}. \end{aligned}$$

Therefore $E$ is a complete set of coset representatives of $\langle (w_1, w_2, \ldots, w_s) \rangle$ in $G$. □

# 4 The Algorithm and Complexity Analysis

In this section, we present an algorithm based on the principles described in the previous section. The analysis of the time and space complexity of the algorithm follows that presented in [EKF00] for the 2-way shuffle.

**The Seed Set Generator for the $(k,n)$-Perfect Shuffle Permutation**

**Step 1** Let $m = kn + 1$ and $S = \emptyset$.

**Step 2** Compute the prime factorisation of $m$, say $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where $p_1 \geq p_2 \geq \cdots \geq p_r$.

**Step 3** For each prime factor $p_i$, compute a primitive root of $p_i$ and call it $g_{i,1}$. If $e_i \geq 2$, compute a primitive root of $p_i^2$ and call it $g_{i,2}$.

**Step 4** For each prime factors $p_i$, compute $w_{i,1} := \operatorname{ind}_{g_{i,1}} k \pmod{p_i}$. If $e_i \geq 2$, compute $w_{i,2} := \operatorname{ind}_{g_{i,2}} 2 \pmod{p_i^2}$.

**Step 5** Compute each divisor of $m$ and its prime factorisation. As a divisor $d$ is generated, carry out steps 5.1 to 5.3.

**Step 5.1** Let the prime factorisation of $d$ be $q_1^{u_1} q_2^{u_2} \cdots q_s^{u_s}$ where $q_1 \geq q_2 \geq \cdots \geq q_s$. For each prime factor $q_i$ of $d$, suppose $j$ is the index such that $q_i = p_j$.
Define $g_i$ as follows: if $u_i = 1$ then $g_i = g_{j,1}$, if $p_j \neq 2$ then $g_i = g_{j,2}$, if $p_j = 2$ and $u_i \geq 2$ then $g_i = g_{j,2}$, otherwise $g_i = 5$. Define $w_i = w_{j,1}$ if $u_i = 1$ or $w_i = w_{j,2}$ if $u_i = 2$. Otherwise, if $p_i \neq 2$, compute $w_i = \operatorname{ind}_{g_i} j \pmod{q_i^{u_i}}$ or if $p_i = 2$ and $u_i \geq 3$, compute and define $w_i, w_i'$ such that $(-1)^{w_i'} 5^{w_i} \equiv j \pmod{2^{u_i}}$.

**Step 5.2** Set $b_0 = 1$. Compute $c_i$ for $i = 1, 2, \ldots, s$ by

$$\begin{aligned}
&t_i = \begin{cases} 2^{u_i - 2}, & \text{if } p_i = 2,\ u_i \geq 3; \\ \varphi(q_i^{u_i}), & \text{otherwise;} \end{cases} \\
&a_i = \gcd(w_i, t_i), \\
&b_i = t_i / a_i, \\
&c_i = a_i \gcd(\operatorname{lcm}(b_0, b_1, b_2, \ldots, b_{i-1}), b_i)
\end{aligned} \tag{6}$$

**Step 5.3** If $q_s \neq 2$, or $q_s = 2$ and $u_s \leq 2$, for every integer vector $(k_1, k_2, \ldots, k_s)$ with $0 \leq k_i < c_i$, solve the system of congruences

$$\begin{cases} x \equiv g_1^{k_1} \pmod{q_1^{u_1}} \\ x \equiv g_2^{k_2} \pmod{q_2^{u_2}} \\ \quad \vdots \\ x \equiv g_s^{k_s} \pmod{q_s^{u_s}} \end{cases} \tag{7}$$

Obtain a solution $x$ in $\{1, 2, \ldots, d\}$ and add $\frac{xm}{d}$ to $S$.
Otherwise, for every integer vector $(k_1, k_2, \ldots, k_s, k_s')$ with $0 \leq k_i < c_i$ and $k_s' = 0, 1$, solve the system of congruences

$$\begin{cases} x \equiv g_1^{k_1} \pmod{q_1^{u_1}} \\ x \equiv g_2^{k_2} \pmod{q_2^{u_2}} \\ \quad \vdots \\ x \equiv g_{s-1}^{k_{s-1}} \pmod{q_{s-1}^{u_{s-1}}} \\ x \equiv (-1)^{k_s'} 5^{k_s} \pmod{2^{u_s}} \end{cases} \tag{8}$$

obtain a solution $x$ in $\{1,2,\ldots,d\}$ and add $\frac{xm}{d}$ to $S$.

**Step 6** Output $S$.

**Proof of Correctness**: If $d$ is not divisible by $2^{u_i}$ with $u_i \geq 3$, by Theorem 2 and equation (7), we know that in step 5.3, each vector $(k_1, k_2, \ldots, k_s)$ with $0 \leq k_i < c_i$ is a coset representative of the quotient

$$(\mathbb{Z}/(\varphi(q_1^{u_1})) \times \mathbb{Z}/(\varphi(q_2^{u_2})) \times \cdots \times \mathbb{Z}/(\varphi(q_s^{u_s})))/\langle(w_1, w_2, \ldots, w_s)\rangle$$

Then the solution of equation (7)

$$x = f^{-1}(h^{-1}((k_1, k_2, \ldots, k_s))) = f^{-1}((g_1^{k_1}, g_2^{k_2}, \ldots, g_s^{k_s}))$$

where $f$ and $h$ are defined by forms (1) and (2) respectively, corresponds to a coset representative of quotient $(\mathbb{Z}/(d))^*/\langle k\rangle_d$ and therefore, $\frac{xm}{d}$ corresponds to a seed of a cycle by Theorem 1.

If $d$ is divisible by $2^{u_s}$, $u_s \geq 3$, then by Theorem 2, each vector $(k_1, \ldots, k_{s-1}, k_s, k'_s)$ with $0 \leq k_i < c_i$ and $k'_s = 0, 1$ corresponds to a coset representative $(k_1, \ldots, k_{s-1}, k_s, k'_s)$ of $\langle(w_1, \ldots, w_{s-1}, w_s, w'_s)\rangle$ in $\mathbb{Z}/(t_1) \times \cdots \times \mathbb{Z}/(t_{s-1}) \times \mathbb{Z}/(t_s) \times \mathbb{Z}/(2)$. Hence it corresponds to a seed $\frac{xm}{d}$ of a cycle, by Theorem 1, since $x = f^{-1}{h'}^{-1}((k_1, \ldots, k_{s-1}, k_s, k'_s))$ where $x$ is the solution of equation (8) and $f$ and $h'$ are defined by the forms (1) and (3) respectively. $\square$

The algorithm just given is a generalisation of that presented in [EKF00]. There it was shown, using some known results regarding the number and distribution of primitive roots, that the entire computation of a seed set for the 2-way shuffle can be accomplished using $O(n)$ arithmetic operations.

The difference between the algorithm for the $k$-way shuffle and that for the 2-way shuffle is in the computation of the indices. We can use the same method for computing $\operatorname{ind}_{g_i} 2$ to compute $\operatorname{ind}_{g_i} k$. We can solve the congruence $(-1)^{w'_i} 5^{w_i} \equiv k \pmod{2^{u_i}}$ using the usual Hensel lifting technique (see for example [VG99]) in $O(u_i^3) = O(kn)$ bit operations. These differences do not increase the overall time complexity of the algorithm. Therefore the more general algorithm can also be realised in time $O(kn)$.

The extra space needed for the variable used by the algorithm is the same as that in [EKF00], so the space complexity is also $O((\log kn)^2)$.

We conclude that a seed set for the $(k,n)$-perfect shuffle permutation can be computed in-place and in time linear in the total number of elements being shuffled. It follows that the $(k,n)$-perfect shuffle permutation can be realised in-place and in linear time by way of a cycle leader algorithm as described in the introduction. We leave as open questions whether or not this result can be used to generalise the 2-way merge algorithm in [EM00] to $k$-way merging and whether or not the space requirement can be further reduced.

# References


[Agn72] J. Agnew. *Explorations in Number Theory.* Brooks/Cole, Monterey, California, 1972.

[Bat91] K. E. Batcher. Decomposition of perfect shuffle networks. In *Proceedings of the 1991 International Conference on Parallel Processing*, volume I, Architecture, pages 255–262, Boca Raton, FL, August 1991. CRC Press.

[BS96] E. Bach and J. Shallit. *Algorithmic Number Theory, Vol 1.* The MIT Press, Cambridge, Mass., 1996.

[DGK83] P. Diaconis, R. L. Graham, and W. Kantor. The mathematics of perfect shuffles. *Advances in Applied Mathematics*, 4(2):175–196, 1983.

[EKF00] J. Ellis, T. Krahn, and H. Fan. Computing the cycles in the perfect shuffle permutation. *Information Processing Letters*, 75:217–224, 2000.

[EM00] J. Ellis and M. Markov. In situ, stable merging by way of the perfect shuffle. *The Computer Journal*, 43(1):40–53, 2000.

[FMP95] Faith E. Fich, J. Ian Munro, and Patricio V. Poblete. Permuting in place. *SIAM Journal on Computing*, 24(2):266–278, 1995.

[Her75] I. N. Herstein. *Topics in Algebra.* Wiley, 1975.

[Jon64] B. W. Jones. *Theory of Numbers, Vol 1.* Holt, Rinehart, Winston, 1964.

[Knu73] D. E. Knuth. *The Art of Computer Programming, vol.3.* Addison-Wesley series in computer science and information processing. Addison-Wesley, 1973.

[Lei92] F. T. Leighton. *Introduction to Parallel Algorithms and Architectures.* Morgan Kaufman, San Mateo, CA., 1992.

[MM87] S. Medvedoff and K. Morrison. Groups of perfect shuffles. *Math. Magazine*, 60(1):3–14, 1987.

[Sto71] H. Stone. Parallel processing with the perfect shuffle. *IEEE Transactions on Computers*, C-20(2):153–161, 1971.

[VG99] Joachim Von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra.* Cambridge University Press, New York, NY, USA, 1999.