Permuting Operations on Strings

—

Their Permutations and Their Primes

Peter R.J. Asveld

Department of Computer Science, Twente University of Technology
P.O. Box 217, 7500 AE Enschede, the Netherlands
e-mail: infprja@cs.utwente.nl

Abstract — We study some length-preserving operations on strings that permute the symbol positions in strings. These operations include some well-known examples (reversal, circular or cyclic shift, shuffle, twist, operations induced by the Josephus problem) and some new ones based on Archimedes spiral. Such a permuting operation X gives rise to a family $\{p(X,n)\}_{n\geq 2}$ of similar permutations. We investigate the structure and the order of the cyclic group generated by such a permutation $p(X,n)$. We call an integer n *X-prime* if $p(X,n)$ consists of a single cycle of length n ($n \geq 2$). Then we show some properties of these X-primes, particularly, how X-primes are related to X'-primes as well as to ordinary prime numbers.

Keywords: operation on strings, shuffle, twist, permutation, cyclic subgroup, prime number, Josephus problem, distribution of prime numbers.

1 Introduction

In theoretical computer science many operations on strings and languages have been investigated. The present paper is devoted to a special class of operations on strings, viz. to length-preserving operations that only permute the symbol positions in the string. In this introductory section we discuss some very simple examples of such operations and we illustrate the properties of the permutations that are associated to these operations. Then in the next few sections we turn our attention to more complicated, and more interesting, length-preserving permuting operations on strings. First, we introduce some notation and terminology.

Let $\mathbb{N}_2 = \{n \in \mathbb{N} \mid n \geq 2\}$, and let $\Sigma_n = \{a_1, a_2, \ldots, a_n\}$ be an alphabet of n different symbols that is linearly ordered by $a_1 < a_2 < \cdots < a_n$ ($n \in \mathbb{N}_2$). The string or word α_n over Σ_n, defined by $\alpha_n = a_1 a_2 \cdots a_n$, is called the *standard word* of length n [19].

Apart from generating the set of all permutations of the standard word as in [2, 5] or some of its subsets [3, 4], there is another area in which permutations and the standard word play an important part. The fact is, some length-preserving operations on strings just permute the symbol positions in the string; so they are permutations actually. This becomes obviously apparent when we apply such an operation X —called *permuting operation* in the sequel— to the standard word α_n.

Example 1.1. (a) Let λ denote the identity operation on strings: $\lambda(a_1a_2a_1a_3) = a_1a_2a_1a_3$ and $\lambda(\alpha_n) = a_1a_2\cdots a_n$.

(b) Consider the transposition of the first two symbols: $\tau(a_1a_2a_1a_3) = a_2a_1a_1a_3$ and $\tau(\alpha_n) = a_2a_1a_3\cdots a_n$.

(c) ρ denotes the *reversal* or *mirror* operation: $\rho(a_1a_2a_1a_3) = a_3a_1a_2a_1$ and $\rho(\alpha_n) = a_na_{n-1}\cdots a_2a_1$.

(d) σ is the *circular* or *cyclic shift*: $\sigma(a_1a_2a_1a_3) = a_2a_1a_3a_1$ and $\sigma(\alpha_n) = a_2a_3\cdots a_na_1$.

Clearly, λ, τ, ρ and σ are permuting operations. □

Such a permuting operation X generates a family $\{p(X,n)\}_{n\geq 2}$ of similar permutations with $p(X,n) \in \mathfrak{S}_n$ where $\mathfrak{S}_n$ is the symmetric group on n elements. Each permutation $p(X,n)$ generates a cyclic subgroup $\langle p(X,n)\rangle$ of $\mathfrak{S}_n$.

Henceforth, permutations will be described by their complete cycle structure representation.

Example 1.1. (continued). (a) $p(\lambda,n) = (1)(2)(3)\cdots(n)$.

(b) $p(\tau,n) = (1\,2)(3)(4)\cdots(n)$.

(c) $p(\rho,n) = (1\ \ n)(2\ \ n{-}1)(3\ \ n{-}2)\cdots(n/2\ \ n/2{+}1)$ if n is even, and
$p(\rho,n) = (1\,n)(2\ \ n{-}1)(3\ \ n{-}2)\cdots((n{-}1)/2\ \ \ (n{+}3)/2)((n{+}1)/2)$ if n is odd.

(d) $p(\sigma,n) = (1\ \ n\ \ n{-}1\ \ n{-}2\ \ \cdots\ \ 3\ \ 2)$. □

Definition 1.2. Let X be a permuting operation on strings. A number n ($n \in \mathbb{N}_2$) is called *X-prime* if $p(X,n)$ consists of a single cycle of length n. The set of X-primes is denoted by $P(X)$. □

Obviously, if a permutation p in $\mathfrak{S}_n$ consists of a cycle of length n, then the order of $\langle p\rangle$, denoted by $\#\langle p\rangle$, equals n. The converse implication does not hold: consider, for instance, the permutation $(1\,2\,3)(4\,5)(6)$ in $\mathfrak{S}_6$ which generates a cyclic subgroup of order 6. Any other perfect number can be used to produce similar counterexamples.

Example 1.1. (continued). (a) $P(\lambda) = \varnothing$. No number n in $\mathbb{N}_2$ is λ-prime.

(b) and (c) Since both τ and ρ are involutions, 2 is the only τ-prime and the only ρ-prime; so $P(\tau) = P(\rho) = \{2\}$.

(d) $P(\sigma) = \mathbb{N}_2$: each n in $\mathbb{N}_2$ is σ-prime. □

Clearly, to obtain non-trivial sets $P(X)$, not all permutations $p(X,n)$ should contain cycles of length less than n for all $n \geq 2$. A first step is to avoid 1-cycles, i.e., fixed points of the mapping $p(X,n) : \{1,\ldots,n\} \to \{1,\ldots,n\}$. So at least, X should disturb each position

in the strings α_n for at least infinitely many numbers n from $\mathbb{N}_2$; cf. (d) and, on the other hand, (a)–(c) in Example 1.1.

In the next sections we focus our attention to some less simple permuting operations on strings. We start with slightly modified versions of the shuffle operation S in Section 2 and of the twist operation T in Section 3. In Section 4 we introduce a few new permuting operations A_0, A_1, A_1^+ and A_1^- based on Archimedes spiral. Section 5 is devoted to the permuting operations J_k that result from the Josephus problem ($k \geq 2$). Duals of permuting operations on strings are studied in Section 6. In these sections we show the results of computer programs that generate the first few X-primes, we comment on the sets $P(X)$ and we investigate the structure of the elements in $\{p(X,n)\}_{n\geq 2}$. We provide answers to questions like "How is $P(X)$ related to $P(X')$ or to the ordinary prime numbers?" with $X, X' \in \{S, T, A_0, A_1, A_1^+, A_1^-, J_2\}$ and $X \neq X'$. Finally, Section 7 contains some concluding remarks and the distributions of S-, T-, A_0-, A_1-, A_1^+-, A_1^-- and J_2-primes.

2 Shuffle

The original (perfect) shuffle operation models the process of cutting a deck of cards into two equal parts and then interleaving these two parts. So applying this shuffle operation S_0 to the standard word α_n results in

$$S_0(\alpha_n) = a_1 a_k a_2 a_{k+1} a_3 a_{k+2} \cdots \qquad \text{where } k = \lceil (n+1)/2 \rceil.$$

Interleaving and shuffling play an important part in describing synchronization aspects of parallel processes; cf. e.g. [16].

Since S_0 leaves the position of the first symbol a_1 of α_n unchanged, we have that $P(S_0) = \varnothing$. The situation becomes less trivial when we modify S_0 slightly: before the interleaving of the two halves of the card deck we interchange the two parts. The resulting shuffle-like permuting operation S is defined by

$$S(\alpha_n) = a_k a_1 a_{k+1} a_2 a_{k+2} a_3 \cdots \qquad \text{where } k = \lceil (n+1)/2 \rceil;$$

cf. §3.4 in [15]. For the permutation $p(S,n)$ induced by the operation S we have

$$\begin{aligned} p(S,n)(m) &= 2m && \text{if } 1 \leq m < k = \lceil (n+1)/2 \rceil, \text{ and} \\ p(S,n)(m) &= 2(m-k)+1 && \text{if } k \leq m \leq n. \end{aligned}$$

So a possible fixed point m_0 of $p(S,n)$ should satisfy $m_0 = 2(m_0 - k) + 1$ or $m_0 = 2k - 1 = 2\lceil (n+1)/2 \rceil + 1$. For n is even, this results in $m_0 = n+1$, which is not meaningful. But for odd n, we get $m_0 = n$. This can also be observed when we look at S: viz. we have for even values of n, that $S(\alpha_n) = a_k a_1 \cdots a_n a_{k-1}$ and $S(\alpha_{n+1}) = a_k a_1 \cdots a_n a_{k-1} a_{n+1}$. Thus, if the permutation $p(S,n)$ can be written as $c_1 c_2 \cdots c_k$ (each c_i is a cycle), then the structure of $p(S, n+1)$ is $c_1 c_2 \cdots c_k (n+1)$. Consequently, all S-prime numbers are even:

$$\begin{aligned} P(S) = \{&2,\ 4,\ 10,\ 12,\ 18,\ 28,\ 36,\ 52,\ 58,\ 60,\ 66,\ 82,\ 100,\ 106,\ 130,\ 138,\ 148,\ 162, \\ &172,\ 178,\ 180,\ 196,\ 210,\ 226,\ 268,\ 292,\ 316,\ 346,\ 348,\ 372,\ 378,\ 388,\ \ldots\}. \end{aligned}$$

This happens to be the integer sequence A071642 in [25].

The mapping $\alpha_n \mapsto a_2a_4\cdots a_na_1a_3\cdots a_{n-1}$ (n is even) and $\alpha_n \mapsto a_2a_4\cdots a_{n-1}a_1a_3\cdots a_n$ (n is odd) is the inverse S^{-1} of S. Note that $P(S^{-1}) = P(S)$.

Example 2.1. For the case $n = 9$, we obtain $S(\alpha_9) = a_5a_1a_6a_2a_7a_3a_8a_4a_9$, $p(S,9) = (1\,2\,4\,8\,7\,5)(3\,6)(9)$, the order of $\langle p(S,9)\rangle$ is 6, and 9 does not belong to $P(S)$. Note that $p(S,8) = (1\,2\,4\,8\,7\,5)(3\,6)$, $\#\langle p(S,8)\rangle = 6$ and $8 \notin P(S)$.

Similarly, we have $S(\alpha_{10}) = a_6a_1a_7a_2a_8a_3a_9a_4a_{10}a_5$, $p(S,10) = (1\,2\,4\,8\,5\,10\,9\,7\,3\,6)$, $\#\langle p(S,10)\rangle = 10$, and hence $10 \in P(S)$. □

Essential in the sequel is the observation that $p(S,n)$ may also be written as

$$\begin{aligned} &p(S,n)(m) \equiv 2m \pmod{n+1} && \text{if } n \text{ is even, and}\\ &p(S,n)(m) \equiv 2m \pmod{n} && \text{if } n \text{ is odd and } 1 \le m < n,\\ &p(S,n)(n) = n && \text{if } n \text{ is odd.} \end{aligned}$$

As a shorthand we write $q_n(m)$ for $p(S,n)(m)$. As $q_n^n(m) = m$, we have for even n,

$$m \cdot 2^n \equiv m \pmod{n+1}, \qquad 1 \le m \le n.$$

Remember that ρ is the reversal or mirror operation (Example 1.1).

Proposition 2.2.

(1) *If n is S-prime, then $m \cdot 2^{n/2} \equiv -m \pmod{n+1}$, where $1 \le m \le n$.*

(2) *If n is S-prime, then $S^{n/2}(w) = \rho(w)$ for each string w of length n.*

Proof. (1) Clearly, n is even and $2^n \equiv 1 \pmod{n+1}$. Consequently, we have that $2^{n/2}$ is an integer with $(2^{n/2})(2^{n/2}) \equiv 1 \pmod{n+1}$. That means that we are looking for solutions of $x^2 \equiv 1 \pmod{n+1}$ under the restriction that there is a single solution only; otherwise we have $\#\langle q_n\rangle < n$ which contradicts the fact that n is S-prime.

Then, according to pp. 128–129 in [12], there exist solutions if $n+1$ is a prime power p^k where $k > 0$. Since $n+1$ is odd, p must be odd as well; so $p > 2$ and $(x-1)(x+1) \equiv 1 \pmod{p^k}$. Now p must divide either $x-1$ or $x+1$ but not both. This implies that we have two candidate solutions:

- $2^{n/2} \equiv +1 \pmod{n+1}$: Then $m \cdot 2^{n/2} \equiv m \pmod{n+1}$, and $\#\langle q_n\rangle = n/2$ which contradicts the S-primality of n.
- $2^{n/2} \equiv -1 \pmod{n+1}$: This is the only remaining possibility, which yields $m \cdot 2^{n/2} \equiv -m \pmod{n+1}$.

(2) From (1) we obtain $q_n^{n/2}(m) \equiv -m \pmod{n+1}$ or, equivalently, $q_n^{n/2}(m) = n+1-m$ which characterizes the reversal operation ρ on strings of even length n. □

Example 2.3. (Card trick). Since 52 is an S-prime, 26 times S-shuffling a deck of 52 cards yields the original card deck in reversed order by Proposition 2.2(2). □

In order to relate S-primes to ordinary prime numbers we need the following result; see, for example, Theorems 2.2.2 (Wilson's Theorem) and 2.2.3 (Converse of Wilson's Theorem) in [20] or Theorem 3.52 in [1].

Theorem 2.4. *The natural number p is an (ordinary) prime number if and only if* $(p-1)! \equiv -1 \pmod{p}$. □

Proposition 2.5. *If n is an S-prime, then $n+1$ is a prime number.*

Proof. Since n is an S-prime number, the residues modulo $n+1$ of 1, 2, 4, ..., 2^{n-1} —i.e., of $q_n^0(1)$, $q_n^1(1)$, $q_n^2(1)$, ..., $q_n^{n-1}(1)$— are equal to 1, 2, 3, ..., n in some order. When we multiply them, we obtain

$$\begin{aligned} n! &\equiv 1 \cdot 2 \cdot 4 \cdots 2^{n-1} && \pmod{n+1} \\ &\equiv \textstyle\prod_{i=0}^{n-1} 2^i && \pmod{n+1} \\ &\equiv 2^{\sum_{i=0}^{n-1} i} && \pmod{n+1} \\ &\equiv 2^{(n/2)(n-1)} && \pmod{n+1} \\ &\equiv (-1)^{n-1} && \pmod{n+1} \\ &\equiv -1 && \pmod{n+1}. \end{aligned}$$

The last two steps follow from Proposition 2.2(1) and from the fact that n is even, respectively. So $n! \equiv -1 \pmod{n+1}$ and $n+1$ is a prime number by Theorem 2.4. □

Apart from fixed points (cycles of length 1) there are of course longer cycles that prevent a number to be S-prime.

Example 2.6. (1) If $n \equiv 2 \pmod 6$, then $p(S,n)$ contains a 2-cycle $((n+1)/3, (2n+2)/3)$. Consequently, each such n unequal to 2 is not S-prime.

Indeed, if $n \equiv 2 \pmod 6$, then both numbers $(n+1)/3$ and $(2n+2)/3$ are integers. Clearly, $q_n((n+1)/3) \equiv 2(n+1)/3 \pmod{n+1}$, i.e., $q_n((n+1)/3) = (2n+2)/3$. Similarly, $q_n((2n+2)/3) \equiv 2(2n+2)/3 \equiv (4n+4)/3 \pmod{n+1}$ holds. Since $n+1 < (4n+4)/3 < 2(n+1)$, we have $q_n((2n+2)/3) = (4n+4)/3 - (n+1) = (n+1)/3$. Hence q_n contains a 2-cycle $(\,(n+1)/3,\ (2n+2)/3\,)$. In a similar way we can prove:

(2) If $n \equiv 6 \pmod{14}$, then $p(S,n)$ contains two 3-cycles $(\,(n+1)/7,\ (2n+2)/7,\ (4n+4)/7\,)$ and $(\,(3n+3)/7,\ (6n+6)/7,\ (5n+5)/7\,)$. So each such n is not S-prime.

(3) If $n \equiv 4 \pmod{10}$, then the 4-cycle $(\,(n+1)/5,\ (2n+2)/5,\ (4n+4)/5,\ (3n+3)/5\,)$ is part of $p(S,n)$. Each such n unequal to 4 is not S-prime. □

The observation that $p(S,n)(m) \equiv 2m \pmod{n+1}$ for even n, and Example 2.6 suggest a characterization of S-primes (Theorem 2.9) for which we recall some terminology (Definition 2.7) and results (Theorem 2.8). As usual $\mathbb{Z}$ denotes the set of all integers.

Definition 2.7. Let $a \in \mathbb{Z}$, and $n \in \mathbb{N}$ with $\gcd(a,n) = 1$.

(1) The *order of* the number *a modulo n*, is the smallest m in $\mathbb{N}$ such that $a^m \equiv 1 \pmod{n}$, denoted $m = \mathrm{ord}(a,n)$.

(2) *Euler's totient function* $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by: $\varphi(n)$ is the number of integers k $(1 \le k < n)$ that are relatively prime to n, i.e. $\gcd(k,n) = 1$.

(3) If $\mathrm{ord}(a,n) = \varphi(n)$, then a is a *primitive root modulo n*. □

The following quite general results can be found in many texts on number theory (cf., e.g., §3.6 of [1], Chapter 3 of [20], or §1.6.7 of [26]); they are included here to show the effect of the special case —viz. primitive roots modulo a prime number— in which we are interested (Theorem 2.9).

Theorem 2.8. *Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$ with $\gcd(a,n) = 1$, and $r = \mathrm{ord}(a,n)$.*

(1) *If $a^m \equiv 1 \pmod{n}$ where $m \in \mathbb{N}$, then $r \mid m$.*

(2) *$r \mid \varphi(n)$.*

(3) *For integers s and t, $a^s \equiv a^t \pmod{n}$ if and only if $s \equiv t \pmod{r}$.*

(4) *No two of the integers a, a^2, a^3, $\cdots$, a^r are congruent modulo r.*

(5) *If m is a positive integer, then the order of a^m modulo n is $\frac{r}{\gcd(r,m)}$.*

(6) *The order of a^m modulo n is r if and only if $\gcd(m,r) = 1$.* □

Theorem 2.9. *A number n is S-prime if and only if $n{+}1$ is an odd prime number with $\mathrm{ord}(2, n{+}1) = n$. Consequently, a number n is S-prime if and only if $n{+}1$ is an odd prime number and 2 is a primitive root modulo $n{+}1$.*

Proof. If n is S-prime, then n is even and by Proposition 2.5 we have that $n{+}1$ is an odd prime number; so $\varphi(n{+}1) = n$. On the other hand, n being S-prime means that n is the smallest number such that $2^n \equiv 1 \pmod{n{+}1}$, i.e., $\mathrm{ord}(2, n{+}1) = n$. Hence 2 is a primitive root modulo $n{+}1$.

Conversely, if $n{+}1$ is an odd prime number and 2 is a primitive root modulo $n{+}1$, then n is even, $\mathrm{ord}(2, n{+}1) = \varphi(n{+}1) = n$, and hence n is the smallest number such that $2^n \equiv 1 \pmod{n{+}1}$, i.e., n is S-prime. □

Let p be a prime number. By $\mathbb{Z}_p$ we denote the finite (or Galois) field of integers modulo p —i.e., $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$— and by $\mathbb{Z}_p^\star$ the cyclic multiplicative group of $\mathbb{Z}_p$. Remember that $\mathbb{Z}_p^\star$ has order $p{-}1$.

If $n{+}1$ is a prime number, then "n is the smallest number such that $2^n \equiv 1 \pmod{n{+}1}$" means that $+2$ generates the multiplicative group $\mathbb{Z}_{n+1}^\star$. Thus we may reformulate Theorem 2.9 as follows.

Theorem 2.10. *A number n is S-prime if and only if $n{+}1$ is an odd prime number and $+2$ generates the multiplicative group $\mathbb{Z}_{n+1}^\star$ of the finite field $\mathbb{Z}_{n+1}$.* □

Example 2.11. (1) For $n = 14$, we have that $n{+}1$ is not prime. So 14 is not S-prime; cf. Example 2.6(1).

(2) If $n = 6$, then $n{+}1$ is prime; but $\mathrm{ord}(2,7) = 3 < 6 = \varphi(7)$. Consequently, 2 is not a primitive root modulo 7 and 6 is not S-prime; cf. Example 2.6(2). The set of possible generators of $\mathbb{Z}_7^\star$ is $\{-2, +3\}$ which does not include $+2$.

(3) Finally, let $n = 12$, then $n{+}1$ is prime, $\mathrm{ord}(2, 13) = 12 = \varphi(12)$, and 12 is S-prime. Indeed, $+2$ is in the set $\{-6, -2, +2, +6\}$ of possible generators of $\mathbb{Z}_{13}^\star$. □

From the many other ways of shuffling a deck of cards we only select one possibility which is, in a certain sense, dual to S. This permuting operation, denoted by $\overline{S}$, models

the process of perfectly shuffling a deck of an even number of cards that has first been put upside down. For an odd number of cards we isolate the last card and put is on top of the shuffled deck[1]:

$$\overline{S}(\alpha_n) = a_{k-1}a_{n-1}a_{k-2}a_{n-2}\cdots a_1a_ka_n \quad \text{if } n \text{ is odd,}$$
$$\overline{S}(\alpha_n) = a_{k-1}a_na_{k-2}a_{n-1}\cdots a_1a_k \quad \text{if } n \text{ is even,}$$

where $k = \lceil (n+1)/2 \rceil$. The corresponding shuffle permutation can be defined by

$$p(\overline{S},n)(m) = n+1-2m \quad \text{if } n \text{ is even and } 1 \le m < k = \lceil (n+1)/2 \rceil,$$
$$p(\overline{S},n)(m) = n-2(m-k) \quad \text{if } n \text{ is even and } k \le m \le n,$$
$$p(\overline{S},n)(m) = n-2m \quad \text{if } n \text{ is odd and } 1 \le m < k = \lceil (n+1)/2 \rceil,$$
$$p(\overline{S},n)(m) = n-1-2(m-k) \quad \text{if } n \text{ is odd and } k \le m < n, \text{ and}$$
$$p(\overline{S},n)(n) = n \quad \text{if } n \text{ is odd,}$$

or rather by

$$p(\overline{S},n)(m) \equiv -2m \pmod{n+1} \quad \text{if } n \text{ is even}$$
$$p(\overline{S},n)(m) \equiv -2m \pmod{n} \quad \text{if } n \text{ is odd and } 1 \le m < n,$$
$$p(\overline{S},n)(n) = n \quad \text{if } n \text{ is odd.}$$

Since for odd n, $p(\overline{S},n)$ has a fixed point (viz. n), all $\overline{S}$-primes are even:

$$P(\overline{S}) = \{4,\ 6,\ 12,\ 22,\ 28,\ 36,\ 46,\ 52,\ 60,\ 70,\ 78,\ 100,\ 102,\ 148,\ 166,\ 172,\ 180,\ 190,$$
$$196,\ 198,\ 238,\ 262,\ 268,\ 270,\ 292,\ 310,\ 316,\ 348,\ 358,\ 366,\ 372,\ 382,\ \ldots\}.$$

This is integer sequence A163776* in [25]. Sequence numbers in [25] which we provided with a star refer to sequences which have been added recently as being new.

Example 2.12. For $n = 7$, we have $\overline{S}(\alpha_7) = a_3a_6a_2a_5a_1a_4a_7$, $p(\overline{S},7) = (1\,5\,4\,6\,2\,3)(7)$, the order of $\langle p(\overline{S},9)\rangle$ is 6, and 7 does not belong to $P(\overline{S})$. Remark that $p(\overline{S},6) = (1\,5\,4\,6\,2\,3)$, $\#\langle p(\overline{S},6)\rangle = 6$ and $6 \in P(\overline{S})$. □

The following results are given without proofs because they are —apart from obvious minus signs— identical to derivations provided earlier in this section.

Proposition 2.13.

(1) *If n is $\overline{S}$-prime, then $m \cdot (-2)^{n/2} \equiv -m \pmod{n+1}$, where $1 \le m \le n$.*

(2) *If n is $\overline{S}$-prime, then $\overline{S}^{n/2}(w) = \rho(w)$ for each string w of length n.* □

Proposition 2.14. *If n is an $\overline{S}$-prime, then $n+1$ is a prime number.* □

Theorem 2.15. *A number n is $\overline{S}$-prime if and only if $n+1$ is an odd prime number with $\mathrm{ord}(-2, n+1) = n$. Consequently, a number n is $\overline{S}$-prime if and only if $n+1$ is an odd prime number and -2 is a primitive root modulo $n+1$.* □

[1] Of course, in playing cards there is probably no application using all cards face up instead of face down. But from a theoretical or mathematical point of view there is no objection to do so.

Theorem 2.16. *A number n is $\overline{S}$-prime if and only if $n{+}1$ is an odd prime number and -2 generates the multiplicative group $\mathbb{Z}^\star_{n+1}$ of the finite field $\mathbb{Z}_{n+1}$.* □

Comparing Theorems 2.15 and 2.16 with Theorems 2.9 and 2.10, respectively, explains why we call the permuting operation $\overline{S}$ dual to S; see also Section 6.

Example 2.17. (1) When $n = 8$, the number $n{+}1$ is not prime. So 8 is not $\overline{S}$-prime.
(2) For $n = 10$, the number $n{+}1$ is prime; but $\mathrm{ord}(-2, 11) = 5 < 10 = \varphi(11)$. Thus -2 is not a primitive root modulo 11 and 10 is not $\overline{S}$-prime. The set of possible generators of $\mathbb{Z}^\star_{11}$ is $\{-5, -4, -3, +2\}$ which does not include -2.
(3) Consider $n = 6$; then $n{+}1$ is prime, $\mathrm{ord}(-2, 7) = 6 = \varphi(7)$, and 6 is $\overline{S}$-prime. Notice that -2 is in the set $\{-2, +3\}$ of possible generators of $\mathbb{Z}^\star_7$. □

3 Twist

The (perfect) twist operation is related to the (perfect) shuffle operation in the following way: before the interleaving process we put the second half of the card deck upside down. Formally, this results in a permuting operation T_0 defined by

$$T_0(\alpha_n) = a_1 a_n a_2 a_{n-1} a_3 a_{n-2} \cdots .$$

Again we have that the position of the first symbol a_1 of α_n is not changed under T_0 and therefore the set of T_0-primes is empty.

As in the previous section we modify T_0 to T by interchanging the two halves of the card deck before shuffling, i.e., T is defined by

$$T(\alpha_n) = a_n a_1 a_{n-1} a_2 a_{n-2} a_3 \cdots .$$

This modified operation T induces a permutation $p(T, n)$ with

$$\begin{aligned} p(T,n)(m) &= 2m && \text{if } 1 \le m < k = \lceil (n+1)/2 \rceil, \text{ and} \\ p(T,n)(m) &= 2(n-m)+1 && \text{if } k \le m \le n. \end{aligned}$$

A possible fixed point m_0 of $p(T, n)$ satisfies $m_0 = 2(n - m_0) + 1$ or $m_0 = (2n + 1)/3$. For $n \ge 2$, integral values of m_0 are obtained by $n = 3k + 1$ $(k \ge 1)$. Hence, the numbers $3k + 1$ $(k \ge 1)$ do not belong to $P(T)$, because $p(T, 3k + 1)$ possesses a fixed point $2k + 1$.

For $P(T)$ we have:

$$\begin{aligned} P(T) = \{&2,\ 3,\ 5,\ 6,\ 9,\ 11,\ 14,\ 18,\ 23,\ 26,\ 29,\ 30,\ 33,\ 35,\ 39,\ 41,\ 50,\ 51,\ 53,\ 65,\ 69,\ 74,\\ &81,\ 83,\ 86,\ 89,\ 90,\ 95,\ 98,\ 99,\ 105,\ 113,\ 119,\ 131,\ 134,\ 135,\ 146,\ 155,\ 158,\\ &173,\ 174,\ 179,\ 183,\ 186,\ 189,\ 191,\ 194,\ 209,\ 210,\ 221,\ \ldots\}. \end{aligned}$$

Example 3.1. We consider the cases for α_6 and α_7: $T(\alpha_6) = a_6 a_1 a_5 a_2 a_4 a_3$, $p(T, 6) = (1\,2\,4\,5\,3\,6)$, and $6 \in P(T)$. And $T(\alpha_7) = a_7 a_1 a_6 a_2 a_5 a_3 a_4$, $p(T, 7) = (1\,2\,4\,7)(3\,6)(5)$, so $\#\langle p(T, 7)\rangle = 4$, and $7 \notin P(T)$. Note that 5 is a fixed point of $p(T, 7)$. □

The elements of $P(T)$ coincide with the so-called Queneau numbers [7]; cf. the sequence A054639 in [25]. These Queneau numbers are usually defined as T^{-1}-primes where T^{-1} is

the inverse of T, i.e., T^{-1} is the mapping defined by $T^{-1} : \alpha_n \mapsto a_2a_4a_6\cdots a_n\cdots a_5a_3a_1$. The permutation $p(T^{-1}, n)$ induced by T^{-1} is defined as follows; cf. [7, 8].

$$p(T^{-1}, n)(m) = m/2 \qquad \text{if } m \text{ is even, and}$$
$$p(T^{-1}, n)(m) = n - (m-1)/2 \qquad \text{if } m \text{ is odd.}$$

Obviously, for $n = 3k + 1$ ($k \geq 1$), the number $2k + 1$ is a fixed point of $p(T^{-1}, n)$ as well.

The twist operation is a major tool in characterizing the behavior of some types of reversal-bounded multipushdown acceptors; see [17, 18]. But there is a much earlier interest in $P(T)$ or rather in $P(T^{-1})$: $p(T^{-1}, n)$ plays an important role in generalizations of a certain verse form called *sextine* or *sestina* in Italian; cf. [22, 23, 8, 10]. The original sextine is based on $p(T^{-1}, 6)$ and consists of six stanzas of six lines each; remember that 6 belongs to the set $P(T^{-1})$.

We will return to the properties of the inverse T^{-1}, the permutations $p(T^{-1}, n)$ and $P(T^{-1})$ later in this section; cf. Theorems 3.5 and 3.6.

Next we turn to k-cycles in $p(T, n)$ for small values of $k \geq 2$; the case $k = 1$ (i.e., the fixed points of $p(T, n)$) has already been discussed above.

Example 3.2. (1) If $n \equiv 2 \pmod 5$, then $p(T, n)$ has a 2-cycle $(\,(2n+1)/5,\ (4n+2)/5\,)$. Each such n unequal to 2 is not T-prime.

(2) If $n \equiv 3 \pmod 7$, then $p(T, n)$ contains a 3-cycles $(\,(2n+1)/7,\ (4n+2)/7,\ (6n+4)/7\,)$. So each such n unequal to 3 is not T-prime.

(3) If $n \equiv 4 \pmod 9$, then $p(T, n)$ contains a 3-cycle $(\,(2n+1)/9,\ (4n+2)/9,\ (8n+4)/9\,)$. And each such n is not T-prime.

As an example we show (3), as the proofs in the other cases are analogous.

The three numbers $(2n+1)/9$, $(4n+2)/9$ and $(8n+4)/9$ are integers by the fact that $n \equiv 4 \pmod 9$. By the definition of $p(T, n)$ we obtain that $p(T, n)((2n+1)/9) = (4n+2)/9$, and $p(T, n)((4n+2)/9) = (8n+4)/9$ as $(4n+2)/9 < \lceil (n+1)/2 \rceil$. Since $(8n+4)/9 \geq \lceil (n+1)/2 \rceil$, we have $p(T, n)((8n+4)/9) = 2(n - (8n+4)/9) + 1 = (2n+1)/9$. Consequently, $p(T, n)$ contains a 3-cycle $(\,(2n+1)/9,\ (4n+2)/9,\ (8n+4)/9\,)$. □

There happens to be a relationship between S-primes, $\overline{S}$-primes and T-primes; viz.

Proposition 3.3.

(1) *For each n in $P(S)$ unequal to 2, the number $n/2$ is in $P(T)$.*

(2) *For each n in $P(\overline{S})$, the number $n/2$ is in $P(T)$.*

Proof. (1) Let n with $n \neq 2$ be in $P(S)$; so n is even. Again we write q_n for $p(S, n)$. We show that there exists an isomorphism φ_n from $\langle p(T, n/2)\rangle$ to $\langle q_n\rangle/_{\cong}$ where the congruence $\cong$ is defined by

$$i \cong j \quad \Longleftrightarrow \quad i \equiv -j \pmod{n+1},$$

and the isomorphism φ_n on $\{1, 2, \ldots, n/2\}$ and its inverse φ_n^{-1} are given by

$\varphi_n(i) = \{i,\ n - i + 1\}$, and

$\varphi_n^{-1}(\{i,k\}) = \min\{i,k\}$,

respectively, with $1 \leq i,k \leq n$. Let $k = \lceil (n+1)/2 \rceil$. Then we have for $1 \leq m \leq n/2$, by the definition of q_n, i.e., of $p(S,n)$, (cf. Section 2),

$$\varphi_n^{-1}\, q_n\, \varphi_n(m) = \varphi_n^{-1}\, q_n(\{m,\ n-m+1\}) = \varphi_n^{-1}(\{q_n(m),\ q_n(n-m+1)\}) =$$
$$= \varphi_n^{-1}(\{2m,\ 2(n-m+1-k)+1\}) = \varphi_n^{-1}(\{2m,\ n-2m+1\}),$$

which is equal to $2m$ if $m < \lceil (n+2)/4 \rceil$, and to $2(\frac{1}{2}n - m) + 1$ if $\lceil (n+2)/4 \rceil \leq m \leq n/2$.

In other words, $\varphi_n^{-1}\, q_n\, \varphi_n(m) = p(T, n/2)(m)$ for each m $(1 \leq m \leq n/2)$. Consequently, if $\langle q_n \rangle$ consists of a single cycle of length n, then $\langle p(T,n/2) \rangle$ consists of a single cycle of length $n/2$. Hence, if n is S-prime, then the number $n/2$ is T-prime.

(2) We proceed as in (1) except that we apply $\overline{q_n} = p(\overline{S}, n)$ instead of q_n and we now define the inverse of φ by

$\varphi_n^{-1}(\{i,k\}) = \max\{i,k\}$.

Then for $1 \leq m \leq n/2$, we have

$$\varphi_n^{-1}\, \overline{q_n}\, \varphi_n(m) = \varphi_n^{-1}\, \overline{q_n}(\{m,\ n-m+1\}) = \varphi_n^{-1}(\{\overline{q_n}(m),\ \overline{q_n}(n-m+1)\}) =$$
$$= \varphi_n^{-1}(\{n+1-2m,\ n-2(n-m+1-k)\}) = \varphi_n^{-1}(\{n+1-2m,\ 2m\}),$$

which equals $2(\frac{1}{2}n - m) + 1$ if $\lceil (n+2)/4 \rceil \leq m \leq n/2$, and $2m$ if $m < \lceil (n+2)/4 \rceil$. If $\langle \overline{q_n} \rangle$ has a single cycle of length n, then $\langle p(T,n/2) \rangle$ has a single cycle of length $n/2$: if n is $\overline{S}$-prime, then $n/2$ is T-prime. □

A comparison of the first few small elements of $P(S)$, respectively $P(\overline{S})$ and $P(T)$ already shows that the converse of Proposition 3.3 does not hold.

Define for each permuting operation X, $H(X)$ by $H(X) = \{n/2 \mid n \in P(X) - \{2\}\}$. Then we have $H(S) \subset P(T)$ and $H(\overline{S}) \subset P(T)$ as well[2]. In Section 7.1 we will show that $P(T) = H(S) \cup H(\overline{S})$.

Crucial in our approach is the fact that the permutation $p(T,n)$ can also be written as

$$p(T,n)(m) \equiv +2m \pmod{2n+1} \qquad \text{if } 1 \leq m < k = \lceil (n+1)/2 \rceil, \text{ and}$$
$$p(T,n)(m) \equiv -2m \pmod{2n+1} \qquad \text{if } k \leq m \leq n.$$

Then the T-counterpart of Propositions 2.2(1) and 2.13(1) reads as follows.

Proposition 3.4. *If n in $\mathbb{N}_2$ is T-prime, then for each m $(1 \leq m < 2n+1)$:*

(1) *If $n \equiv 1 \pmod 4$, then $m \cdot 2^n \equiv -m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv +m \pmod{2n+1}$.*

(2) *If $n \equiv 2 \pmod 4$, then $m \cdot 2^n \equiv -m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv -m \pmod{2n+1}$.*

(3) *If $n \equiv 3 \pmod 4$, then $m \cdot 2^n \equiv +m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv -m \pmod{2n+1}$.*

Proof. If we apply the permutation $p(T,n)$ iteratively n times to m, then we encounter all values $1, 2, \ldots, n$ in some order and $p^n(T,n)(m) = m$, as n is T-prime.

(1) If $n = 4k+1$ $(k \geq 1)$, then we have in this sequence of length n in total: $2k$ multiplications by $+2$ (viz. in case we apply $p(T,n)$ to a number strictly less than

[2]We use "$\subseteq$" for set inclusion and "$\subset$" for proper inclusion.

$\lceil (n+1)/2 \rceil$) and $2k{+}1$ multiplications by -2 (viz. when we apply $p(T,n)$ to a number greater than or equal to $\lceil (n+1)/2 \rceil$) both modulo $2n{+}1$. Consequently, as $2k{+}1$ is odd, we obtain $m \cdot 2^n \equiv -m \cdot 2^{2k} \cdot (-2)^{2k+1} \equiv -m \,(\mathrm{mod}\ 2n{+}1)$. But then we have $m \cdot (-2)^n \equiv m \cdot 2^n \cdot (-1)^{4k+1} \equiv +m \,(\mathrm{mod}\ 2n{+}1)$.

(2) If $n = 4k{+}2$ ($k \geq 1$), then we apply $2k{+}1$ multiplications by $+2$ and $2k{+}1$ multiplications by -2 modulo $2n{+}1$. Then we have $m \cdot 2^n \equiv -m \cdot 2^{2k+1} \cdot (-2)^{2k+1} \equiv -m \,(\mathrm{mod}\ 2n{+}1)$ and $m \cdot (-2)^n \equiv -m \cdot 2^n \cdot (-1)^{4k+2} \equiv -m \,(\mathrm{mod}\ 2n{+}1)$.

(3) If $n = 4k{+}3$ ($k \geq 0$), then we use $2k{+}1$ multiplications by $+2$ and $2k{+}2$ multiplications by -2 modulo $2n{+}1$. Hence $m \cdot 2^n \equiv m \cdot 2^{2k+1} \cdot (-2)^{2k+2} \equiv +m \,(\mathrm{mod}\ 2n{+}1)$ and $m \cdot (-2)^n \equiv m \cdot 2^n \cdot (-1)^{4k+3} \equiv -m \,(\mathrm{mod}\ 2n{+}1)$. □

Note that the case $n \equiv 0 \,(\mathrm{mod}\ 4)$ is not included in Proposition 3.4. It turns out that if $n \equiv 0 \,(\mathrm{mod}\ 4)$, then n is not T-prime; see [7] or Theorem 3.13 below.

Remember that, for a prime number p, $\mathbb{Z}_p^\star$ denotes the cyclic multiplicative group of order $p{-}1$ of the finite field $\mathbb{Z}_p$.

In [7] a partial characterization of T^{-1}-primes has been established. Since $P(T) = P(T^{-1})$, it also applies to T-primes. Reformulated in terms of T-primes it reads as follows.

Theorem 3.5. [7] *Let n be a number in $\mathbb{N}_2$.*

(1) *If n is T-prime, then $2n{+}1$ is a prime number.*

(2) *If $2n{+}1$ is a prime number and $+2$ generates the multiplicative group $\mathbb{Z}_{2n+1}^\star$ of $\mathbb{Z}_{2n+1}$, then n is T-prime.*

(3) *If both n and $2n{+}1$ are prime numbers, then n is T-prime.*

(4) *If n is of the form $n = 2p$ where p and $4p{+}1$ are prime numbers ($p \geq 3$), then n is T-prime.*

(5) *Numbers of the form 2^k ($k \geq 2$), $2^k - 1$ ($k \geq 3$), and $4k$ ($k \geq 1$) are not T-prime.* □

Earlier we observed that numbers of the form $3k+1$ ($k \geq 1$) are not T-prime as they are fixed points of $p(T,n)$. Note that this easily follows from Theorem 3.5(1).

A complete characterization of $P(T^{-1})$ is given in [8]; notice that in [8] there is no reference to [7]. The main result from [8] reads, slightly reformulated[3], as follows.

Theorem 3.6. [8] *A number n in $\mathbb{N}_2$ is T-prime if and only if*

(1) *$2n{+}1$ is a prime number, and*

(2) *at least one of -2 and $+2$ is a generator of the multiplicative group $\mathbb{Z}_{2n+1}^\star$ of $\mathbb{Z}_{2n+1}$.* □

The remaining part of this section is devoted to a complete, more refined, characterization of T-primes (Theorem 3.15 below), from which we obtain the main results of [7] and [8] as particular instances.We phrase our characterization and its proof in terms of T, $p(T,n)$ and $P(T)$ rather than using T^{-1}, $p(T^{-1},n)$ and $P(T^{-1})$; cf. Theorem 3.15.

[3] In [8] condition (2) reads: "either $+2$ or -2 is a generator of the multiplicative group $\mathbb{Z}_{2n+1}^\star$ of $\mathbb{Z}_{2n+1}$.". If "either $\cdots$ or $\cdots$" stands for the *exclusive or*, then this version of the result is definitely wrong; cf. our characterizations in Theorem 3.15 and Section 4 below. This poor formulation of the main result in [8] probably stems from its sloppy proof (inaccurate use of minus signs).

The first step is Lemma 3.7 which has originally been conjectured by R. Queneau[22, 23]; this lemma and Proposition 3.8 have been proven in [8].

Lemma 3.7. [8] *If there exist integers x and y with $x, y \geq 1$ such that $n = 2xy + x + y$, then n is not T-prime.*

Proof. Suppose there exist integers $x, y \geq 1$ such that $n = 2xy + x + y$. Then $2x + 1 < n$. We consider the multiples of $2x + 1$ that are less than or equal to n and their images under the permutation $p(T, n)$.

For multiples $m(2x + 1)$ with $1 \leq m(2x + 1) < \lceil (n + 1)/2 \rceil$ and with $\lceil (n + 1)/2 \rceil \leq m(2x + 1) \leq n$, we have respectively,

$$\begin{aligned} p(T,n)(m(2x+1)) &= 2m(2x+1), \\ p(T,n)(m(2x+1)) &= 2(n - m(2x+1)) + 1 \\ &= 2(2xy + x + y - 2mx - m) + 1 \\ &= 4xy + 2y - 4mx - 2m + 2x + 1 \\ &= (2x+1)(2y - 2m + 1). \end{aligned}$$

Clearly, every multiple of $2x + 1$ is mapped by $p(T, n)$ on another multiple of $2x + 1$. For n to be T-prime, $p(T, n)$ must consists of a single cycle of length n, which implies that all numbers l with $1 \leq l \leq n$ must be divisible by $2x + 1$. But this is impossible since $2x + 1 > 1$ for $x \geq 1$. □

Proposition 3.8. [8] *If n is T-prime, then $2n + 1$ is a prime number.*

Proof. Assume to the contrary that $2n + 1$ is not prime. Since $2n + 1$ is an odd integer, it must be the product of two odd integers strictly greater than 1:

$(2x + 1)(2y + 1) = 2n + 1$, with $x, y \geq 1$.

This yields $4xy + 2x + 2y + 1 = 2n + 1$, or $2xy + x + y = n$. From Lemma 3.7 it then follows that n is not T-prime. □

In order to establish our characterization (Theorems 3.13 and 3.15), we need a definition and a few results from number theory; see, for example, Theorem 95 in [14], Theorem 3.103 in [1], §4.1 in [20] or §1.6.6 in [26].

Definition 3.9. Let p be an odd prime number. The number a is a *quadratic residue of p* if the congruence $x^2 \equiv a \pmod{p}$ has a solution. When no such solution exists, the number a is called a *quadratic non-residue of p*. □

Proposition 3.10. $+2$ *is a quadratic residue of primes of the form $8k \pm 1$ and a quadratic non-residue of primes of the form $8k \pm 3$.* □

We also need a companion of Proposition 3.10 —viz. Proposition 3.12— the proof of which is a modification of the argument used in establishing Theorem 95 in [14] (Proposition 3.10); we use some additional notation and Gauss's lemma (Lemma 3.11).

Let p be an odd prime and a any number not divisible by p. Then *Legendre's symbol* (a/p) is defined by

$(a/p) = +1$ if a is a quadratic residue of p, and

$(a/p) = -1$ if a is a quadratic non-residue of p.

Lemma 3.11: Gauss's lemma. *$(a/p) = (-1)^{\mu}$, where μ is the number of members in the set $S(a,p) = \{a, 2a, 3a, \ldots, \frac{1}{2}(p-1)a\}$ whose least positive residues* (mod p) *are greater than $\frac{1}{2}p$.* □

Proposition 3.12. *-2 is a quadratic residue of primes of the form $8k+1$ and $8k+3$, and a quadratic non-residue of primes of the form $8k+5$ and $8k+7$.*

Proof. For $a = -2$, the members of the set $S(a,p)$ are $-2, -4, -6, \ldots, -p+1$. We can rearrange these residues in the following way:

$$r_1, r_2, \ldots, r_\lambda, \quad -s_1, -s_2, \ldots, -s_\mu,$$

where $\lambda + \mu = \frac{1}{2}(p-1)$, $0 < r_i < \frac{1}{2}p$ $(1 \le i \le \lambda)$, $0 < s_j < \frac{1}{2}p$ $(1 \le j \le \mu)$.

Now μ is the number of positive even integers less than $\frac{1}{2}p$; that means $\mu = [\frac{1}{4}p]$, i.e., μ equals the largest integer which does not exceed $\frac{1}{4}p$.

If $p \equiv 1 \,(\mathrm{mod}\ 4)$, then $\mu = (p-1)/4$ and if $p \equiv 3 \,(\mathrm{mod}\ 4)$, then $\mu = (p-3)/4$.

Thus if $p = 8k+1$ or $p = 8k+5$, then we have $\mu = 2k$ or $\mu = 2k+1$, respectively. From Gauss's lemma it follows that $(-2/(8k+1)) = +1$ and $(-2/(8k+5)) = -1$.

Similarly, if $p = 8k+3$ or $p = 8k+7$, then we obtain $\mu = 2k$ or $\mu = 2k+1$, respectively. Gauss's lemma now implies that $(-2/(8k+3)) = +1$ and and $(-2/(8k+7)) = -1$. □

For an alternative proof of Proposition 3.12 we refer to Example 4.1.18 in [20].

We now turn to a result from [7] —viz. the third part of Theorem 3.5(5)— and its proof: they play a more important role here than in [7].

Theorem 3.13. [7] *Let n be a number in $\mathbb{N}_2$. If $n \equiv 0 \,(\mathrm{mod}\ 4)$, then n is not T-prime.*

Proof. Assume to the contrary that n, with $n = 4k$ for some $k \ge 1$, is T-prime. Then Proposition 3.8 implies that $2n+1 = 8k+1$ is a prime number p. By Proposition 3.10, the number $+2$ is a quadratic residue of p; so there exists an x with $x^2 \equiv 2 \,(\mathrm{mod}\ p)$.

However, for each x we have $x^{2n} \equiv 1 \,(\mathrm{mod}\ p)$, and so $2^{4k} \equiv 2^n \equiv x^{2n} \equiv 1 \,(\mathrm{mod}\ p)$. Then $(2^{2k}+1)(2^k+1)(2^k-1) \equiv 0 \,(\mathrm{mod}\ p)$ holds, which implies that $2^{2k} \equiv -1 \,(\mathrm{mod}\ p)$ or $2^k \equiv -1 \,(\mathrm{mod}\ p)$ or $2^k \equiv 1 \,(\mathrm{mod}\ p)$. In each of these three cases we have that the absolute value of $p^t(T,n)(2)$ equals 1 where t is equal to $2k-1$, $k-1$ and $k-1$, respectively. Then $p^{2t+1}(T,n)(2) = 2$, and as in each of these three cases $2t+1 < 4k = n$, this contradicts the assumption that n is T-prime. □

In the sequel we will sometimes represent $\mathbb{Z}_{2n+1}$ by $\mathbb{A}_n = \{-n, -n+1, \ldots, 0, 1, \ldots, n\}$ in which $n+1, n+2, \ldots, 2n$ are represented by $-n, -n+1, \ldots, -1$, respectively; cf. [7]. $\mathbb{A}_n$ is provided with a product (in $\mathbb{Z}$ modulo $2n+1$) and an absolute value by

$|u| = +u$ if $0 \le u \le n$, and

$|u| = -u$ if $-n \le u \le 0$.

For this absolute value we have $|uv| = ||u||v||$; cf. [7] for details.

Next we define for each $p(T,n)$ a corresponding permutation q_n which uses $\mathbb{A}_n$ instead of $\mathbb{Z}_{2n+1}$:

$$q_n(m) \mathbin{\mathring{=}} 2m \qquad \text{if } 1 \le m < k = \lceil (n+1)/2 \rceil, \text{ and}$$
$$q_n(m) \mathbin{\mathring{=}} |2m| \qquad \text{if } k \le m \le n.$$

We use the $\mathring{=}$-symbol to emphasize that multiplications and their results should be considered with respect to $\mathbb{A}_n$ rather than to $\mathbb{Z}_{2n+1}$. Then we have, for instance, $q_n(m) \mathbin{\mathring{=}} |2m|$ and, more generally, $q_n^t(m) \mathbin{\mathring{=}} |2^t m|$ for $1 \le m \le n$ and $t \ge 1$.

Example 3.14. If $n = 5$ and we apply $p(T, 5)$ to its respective arguments $(1, 2, 3, 4, 5)$, we obtain $(2, 4, 5, 3, 1)$. Alternatively, we compute q_5 by multiplying its respective arguments by 2, which yields $(2, 4, 6, 8, 10)$ in $\mathbb{Z}_{11}$ and $(2, 4, -5, -3, -1)$ in $\mathbb{A}_5$. Taking absolute values results in $q_5 = p(T, 5)$.

Similarly, for q_5^4 we multiply by 16 yielding $(16, 32, 48, 64, 80)$ in $\mathbb{Z}$, $(5, 10, 4, 9, 3)$ in $\mathbb{Z}_{11}$ and $(5, -1, 4, -2, 3)$ in $\mathbb{A}_5$; the absolute values are $(5, 1, 4, 2, 3)$. Hence $q_5^4 = p(T^{-1}, 5)$. □

We are now ready for the characterization of T-primes.

Theorem 3.15. *A number n in $\mathbb{N}_2$ is T-prime if and only if $2n+1$ is a prime number and exactly one of the following three conditions holds:*

(1) $n \equiv 1 \pmod 4$ *and $+2$ is a generator of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$, but -2 is not.*

(2) $n \equiv 2 \pmod 4$ *and both -2 and $+2$ are generators of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

(3) $n \equiv 3 \pmod 4$ *and -2 is a generator of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$, but $+2$ is not.*

Proof. Suppose n in $\mathbb{N}_2$ is a T-prime; then by Proposition 3.8 the number $p = 2n+1$ is an odd prime number. The multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$, consisting of the numbers 1, 2 ..., $p-1$, is cyclic. Since the order of $\mathbb{Z}^\star_{2n+1}$ equals $p-1 = 2n$, we have for each x in $\mathbb{Z}^\star_{2n+1}$ that $x^{2n} \equiv 1 \pmod p$; cf. Fermat's little theorem.

From Theorem 3.13 we know that n is equal to 1, 2 or 3 modulo 4; let g be equal to $+2$, -2 or $+2$, and -2, respectively. Assume to the contrary that g does not generate $\mathbb{Z}^\star_{2n+1}$. Since $g^{2n} \equiv 1 \pmod p$, we must have that $g^2 \equiv 1 \pmod p$ or $g^d \equiv 1 \pmod p$ for some divisor d of n. Now the first alternative $g^2 \equiv 1 \pmod p$ is impossible because $g^2 \equiv 4 \pmod p$ whenever $n \ge 2$. The second alternative implies that $g^n \equiv 1 \pmod p$ as well, which contradicts Proposition 3.4 for $m = 1$. Hence g generates $\mathbb{Z}^\star_{2n+1}$.

If $n \equiv 1 \pmod 4$, then $n = 4k+1$ and $p = 8k+3$ for some $k \ge 1$. Then by Proposition 3.12, -2 is a quadratic residue of p: there is an x with $x^2 \equiv -2 \pmod p$. As $x^{2n} \equiv 1 \pmod p$ holds for each x in $\mathbb{Z}^\star_{2n+1}$, this implies $x^{2n} \equiv (-2)^n \equiv 1 \pmod p$. But this means that -2 has order n at most (cf. Proposition 3.4(1) with $m = 1$) instead of $2n$; hence -2 does not generate $\mathbb{Z}^\star_{2n+1}$.

If $n \equiv 3 \pmod 4$, then $n = 4k+3$ and $p = 8k+7$ for some $k \ge 0$. Now Proposition 3.10 implies that $+2$ is a quadratic residue of p, which yields in a similar way that $+2$ has order n at most (cf. also Proposition 3.4(3) with $m = 1$), and that $+2$ does not generate $\mathbb{Z}^\star_{2n+1}$.

Conversely, if $2n+1$ is a prime number, then $\mathbb{Z}_{2n+1}$ is a finite field of which its multiplicative group $\mathbb{Z}^\star_{2n+1}$ possesses $2n$ elements.

Let g be equal to $+2$ (1), -2 or $+2$ (2), and -2 (3), respectively, and consider

$g^1,\ g^2,\ \ldots\ ,\ g^{n-1},\ g^n,\ g^{n+1},\ \ldots\ ,\ g^{2n}$

in $\mathbb{A}_n$. Since g generates $\mathbb{Z}^\star_{2n+1}$ all these elements in the sequence are different and $g^{2n} \triangleq +1$. As $q^t_n(m) \triangleq |2^t m|$ for each m $(1 \leq m \leq n)$, the absolute values of the first n elements in this sequence coincide with the sequence

$q^1_n(1),\ q^2_n(1),\ \ldots\ ,\ q^n_n(1).$

Now $q^n_n(1) \triangleq 1$, which implies that $|g^n| \triangleq 1$ or, equivalently, that either $g^n \triangleq +1$ or $g^n \triangleq -1$. But $g^n \triangleq +1$ is impossible, as it would mean that $\mathbb{Z}^\star_{2n+1}$ possesses at most n elements rather than $2n$. Hence we have that $g^n \triangleq -1$.

Assume that $\#\langle q_n\rangle < n$. This implies the existence of an i and a j $(1 \leq i < j \leq n)$ such that $q^i_n(1) \triangleq q^j_n(1)$ or, equivalently, $g^i \triangleq -g^j$ in $\mathbb{A}_n$. As $g^n \triangleq -1$ we then obtain that $g^{n+i} \triangleq g^j$ in $\mathbb{A}_n$ with $j < n + i$, which contradicts the fact that g generates $\mathbb{Z}^\star_{2n+1}$. Consequently, $\#\langle p(T, n)\rangle = \#\langle q_n\rangle = n$, i.e., n is T-prime. □

Example 3.16. (1) We have $7 \notin P(T)$, since 15 is not a prime number; cf. Examples 3.1 and 3.2(1).

(2) The number 8 is also not T-prime; although 17 is a prime number, both $+2$ and -2 fail to be a generator of the multiplicative group $\mathbb{Z}^\star_{17}$ of $\mathbb{Z}_{17}$. But each element from $\{-7, -6, -5, -3, +3, +5, +6, +7\}$ is a generator of this cyclic group $\mathbb{Z}^\star_{17}$.

(3) For $n = 9$, we have that 19 is a prime number and the set of possible generators of $\mathbb{Z}^\star_{19}$ is $\{-9, -6, -5, -4, +2, +3\}$; this set includes $+2$ and so $9 \in P(T)$.

(4) In case $n = 6$, we obtain that the set of possible generators of $\mathbb{Z}^\star_{13}$ is $\{-6, -2, +2, +6\}$, which includes both $+2$ and -2, and so 6 is T-prime; cf. Example 3.1.

(5) Finally, $3 \in P(T)$ as both 7 is a prime number and -2 generates $\mathbb{Z}^\star_7$; cf. Example 3.2(2). The set of possible generators of $\mathbb{Z}^\star_7$ is $\{-2, +3\}$. □

Now Theorem 3.6 (the main result from [8]) is a corollary of Theorem 3.15. And some main results from [7] also follow from our characterization of T-primes: cf. Theorem 3.5(1), 3.5(2) and the third part of 3.5(5). Notice that the first part of Theorem 3.5(5) is a consequence of its third part; cf. Theorem 3.13.

Reference [10], which does refer to [7] but not to [8], includes two characterizations of $P(T^{-1})$ (viz. Theorem 2 and Corollary 1 in [10]): If $n \in \mathbb{N}$ and $p = 2n+1$, then

• n is T^{-1}-prime if and only if p is a prime number and either 2 is of order $2n$ in $\mathbb{Z}/p\mathbb{Z}$, or n is odd and 2 is of order n in $\mathbb{Z}/p\mathbb{Z}$, and

• n is T^{-1}-prime if and only if p is a prime number and either 2 is of order $2n$ in $\mathbb{Z}/p\mathbb{Z}$ and $n \equiv 1$ or 2 (mod 4), or 2 is of order n in $\mathbb{Z}/p\mathbb{Z}$ and $n \equiv 3$ (mod 4),

from which it is possible [11] to infer Theorem 4.15 as well.

For completeness' sake we include here (slightly modified) proofs from [7] of the remaining statements of Theorem 3.5.

Proof of Theorem 3.5(3). Let both n and $2n+1$ $(n \in \mathbb{N}_2)$ be prime numbers. The case $n = 2$ is trivial; so we assume that n is an odd prime number. We distinguish two cases:

• $n = 4k{+}1$ ($k \geq 1$). From $2^{2n} \equiv 1 \pmod{2n{+}1}$, we obtain $(2^n{-}1)(2^n{+}1) \equiv 0 \pmod{2n{+}1}$. If $2^n{-}1 \equiv 0 \pmod{2n{+}1}$, then $2^{n+1} \equiv 2 \equiv 2^{4p+2} \equiv (2^{2p+1})^2 \pmod{2n{+}1}$ which contradicts $(+2/(8k+3)) = -1$; cf. Proposition 3.10. Hence we have $2^n \equiv -1 \pmod{2n{+}1}$ and $2^{2n} \equiv 1 \pmod{2n{+}1}$. This latter congruence implies that the order of 2 is a divisor of $2n$, i.e., it equals either $2n$, n or 2 as n is a prime number. It is not equal to n (because $2^n \equiv -1 \pmod{2n{+}1}$ and to 2 (because $2^2 - 1 \equiv 0 \pmod{2n{+}1}$, implies that $n = 1$). So the order of 2 is $2n$ and $+2$ generates $\mathbb{Z}^\star_{2n+1}$. Theorem 3.15 now yields that n is T-prime.

• $n = 4k + 3$ ($k \geq 0$). In a way similar to the previous case, we infer from $(-2)^{2n} \equiv 1 \pmod{2n{+}1}$ that $(-2/(8k + 7)) = +1$ which contradicts Proposition 3.12; we then obtain that -2 generates $\mathbb{Z}^\star_{2n+1}$ and that, by Theorem 3.15, n is T-prime[4]. □

Proof of Theorem 3.5(4). If p is an odd prime with $p = 2k{+}1$ ($k \geq 1$), then we have $2n{+}1 = 4p{+}1 = 8k{+}5$. Now $2^{2n} \equiv 1 \pmod{4p{+}1}$, which implies $2^{4p} \equiv 1 \pmod{4p{+}1}$ or, equivalently, $2^{4p} - 1 \equiv (2^{2p}{+}1)(2^p{+}1)(2^p{-}1) \equiv 0 \pmod{4p{+}1}$.

If $2^p \equiv 1 \pmod{4p{+}1}$, then $2 \equiv 2^{p+1} \equiv 2^{2(k+1)} \pmod{4p{+}1}$ and $(+2/(4p{+}1)) = (+2/(8k{+}5)) = +1$, which contradicts Proposition 3.10.

If $2^p \equiv -1 \pmod{4p{+}1}$, then $-2 \equiv 2^{p+1} \equiv 2^{2(k+1)} \pmod{4p{+}1}$ and $(-2/(4p{+}1)) = (+2/(8k{+}5)) = +1$, which contradicts Proposition 3.12.

Consequently, we have $2^{2p} \equiv -1 \equiv 2^n \pmod{4p{+}1}$, which implies $2^{4p} \equiv 1 \pmod{4p{+}1}$. So the order of 2 is a divisor of $4p$, i.e., it equals either $4p$, $2p$, p, 4 or 2.

This divisor is unequal to p and $2p$ (as shown above) and to 2, because $2^2{-}1 \equiv 0 \pmod{2n{+}1}$ implies $n = 1$. It is also unequal to 4, as $2^4{-}1 \equiv 0 \pmod{2n{+}1}$ implies that the prime $2n{+}1$ should divide 15, i.e., $2n{+}1 = 3$ with $n = 1$ or $2n{+}1 = 5$ with $n = 2$.

The remaining case —viz. the divisor equals $4p = 2n$— means that 2 has order $2n$, i.e., that $+2$ generates $\mathbb{Z}^\star_{2n+1}$ and, by Theorem 3.15, that n is T-prime. □

Proof of Theorem 3.5(5). As remarked above, the only statement left to be proved is the second one from Theorem 3.5(5). Let n be equal to $2^k - 1$ with $k \geq 3$ and consider the sequence

$$q_n^0(2) \doteq 2,\ q_n^1(2) \doteq 2^2,\ \cdots,\ q_n^{k-1}(2) \doteq |2^k| \doteq n,\ q_n^k(2) \doteq 1,\ q_n^{k+1}(2) \doteq 2$$

in $\mathbb{A}_n$. Thus the cycle generated by 2 in q_n —and in $p(T, N)$, of course— has length $k{+}1$. Since $k{+}1 < 2^k - 1 = n$ for $k \geq 3$, this implies that n is not T-prime. □

Apart from the results collected in Theorem 3.5, [7] includes some other interesting results, particularly with respect to the structure of $p(T, n)$:

• If c_1 is the cycle that contains 2, then the length of any other cycle in $p(T, n)$ divides the length of c_1. Consequently, $\#\langle p(T, n)\rangle$ equals the length of c_1.

• If $2n + 1$ is a prime number, then all cycles in $p(T, n)$ have the same length, and that length is a divisor of n.

We conclude this section with a warning: we cannot simply substitute "+2 generates $\mathbb{Z}^\star_{2n+1}$" by "$(+2/(2n{+}1)) = -1$" and "-2 generates $\mathbb{Z}^\star_{2n+1}$" by "$(-2/(2n{+}1)) = -1$"

[4] In [7] a direct ad hoc argument is used in this case instead of applying Proposition 3.12 as we do.

in Theorem 3.15 (as the very naive reader probably may think), and still have a valid characterization of T-primes.

For $n \equiv 1 \pmod 4$, the smallest counterexample is $n = 21$; then $2n+1 = 43$ is a prime number, $(+2/43) = -1$, but $+2$ (and -2) do not belong to the set $\{-17, -15, -14, -13, -10, -9, +3, +5, +12, +18, +19, +20\}$ of possible generators of $\mathbb{Z}_{43}^\star$.

If $n \equiv 2 \pmod 4$, then the smallest counterexample is $n = 54$: $2n+1 = 109$ is a prime, $(-2/109) = (+2/109) = -1$, but neither -2 nor $+2$ are in the set $\{\pm 6, \pm 10, \pm 11, \pm 13, \pm 14, \pm 18, \pm 24, \pm 30, \pm 37, \pm 39, \pm 40, \pm 42, \pm 44, \pm 47, \pm 50, \pm 51, \pm 52, \pm 53\}$ of possible generators of $\mathbb{Z}_{109}^\star$.

In case $n \equiv 3 \pmod 4$, the smallest counterexample is $n = 15$: $2n+1 = 31$ is a prime number, $(-2/31) = -1$, but -2 (and $+2$) are not member of the set $\{-14, -10, -9, -7, +3, +11, +12, +13\}$ of possible generators of $\mathbb{Z}_{31}^\star$.

The prime numbers p satisfying the property, that $+g$ generates $\mathbb{Z}_p^\star$ if and only if $-g$ does so, are

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, ...;

they are the Pythagorean primes; cf. A002144 in [25]. Clearly, if n is T-prime with $n \equiv 2 \pmod 4$, then $2n+1$ is a Pythagorean prime, but the converse does not hold. The smallest counterexample is $n = 8$, not being a T-prime, whereas 17 is a Pythagorean prime. And, indeed, $n = 54$ with Pythagorean prime 109 is the smallest counterexample with $n \equiv 2 \pmod 4$.

4 Archimedes

In this section we introduce a few new permuting operations on strings, denoted by A_0, A_1, A_1^+ and A_1^-, which are based on Archimedes spiral.

Consider an Archimedes spiral with polar equation $r = c\,\theta$ ($c > 0$; θ is the angle) where $\theta \geq 0$. We place the first symbol a_1 from the standard word α_n at the origin ($\theta = 0$) and each time, as θ increases, that r intersects the X-axis (in the XY-plane) we put the next symbol from α_n on the X-axis. Finally, reading the symbols placed on the X-axis from left to right yields $A_0(\alpha_n)$. Thus we have

$$A_0(\alpha_n) = a_n a_{n-2} \cdots a_4 a_2 a_1 a_3 a_5 \cdots a_{n-3} a_{n-1} \qquad \text{if } n \text{ is even, and}$$

$$A_0(\alpha_n) = a_{n-1} a_{n-3} \cdots a_4 a_2 a_1 a_3 a_5 \cdots a_{n-2} a_n \qquad \text{if } n \text{ is odd.}$$

The corresponding permutation $p(A_0, n)$ satisfies

$$p(A_0, n)(m) = \lceil (n+1)/2 \rceil + (-1)^{m-1} \lceil (m-1)/2 \rceil, \qquad 1 \leq m \leq n.$$

For odd m this yields $p(A_0, n)(m) = \lceil (n+1)/2 \rceil + (m-1)/2$ and for a possible fixed point m_0, we have $m_0 = 2\lceil (n+1)/2 \rceil - 1$. For n is even, we then get $m_0 = n+1$ which is meaningless, and for n is odd, this yields $m_0 = n$ which is already obvious from A_0 as it does not affect the position of a_n in α_n. Therefore all A_0-prime numbers are even.

For even values of m, $p(A_0, n)(m) = \lceil (n+1)/2 \rceil - m/2$ and $m_0 = \frac{2}{3}\lceil (n+1)/2 \rceil$. This implies that for n equal to $6k+4$ and $6k+5$ ($k \geq 0$), $p(A_0, n)$ has a fixed point.

Hence all odd numbers and all numbers $6k+4$ ($k \geq 0$) are not in $P(A_0)$:

$P(A_0) = \{2, 6, 14, 18, 26, 30, 50, 74, 86, 90, 98, 134, 146, 158, 174, 186, 194, 210,$
$230, 254, 270, 278, 306, 326, 330, 338, 350, 354, 378, 386, 398, 410, \ldots\}$;

cf. sequence A163777* in [25].

Example 4.1. $A_0(\alpha_5) = a_4a_2a_1a_3a_5$, $p(A_0, 5) = (1\,3\,4)(2)(5)$, $\#\langle p(A_0, 5)\rangle = 3$, and $5 \notin P(A_0)$. Similarly, $A_0(\alpha_6) = a_6a_4a_2a_1a_3a_5$, $p(A_0, 6) = (1\,4\,2\,3\,5\,6)$, and $6 \in P(A_0)$. □

As a variation of A_0, define A_1 by starting with the Archimedes-like spiral defined by the polar equation $r = c(\theta + \pi)$ with $\theta \geq 0$ rather than by $r = c\,\theta$. Then we have

$A_1(\alpha_n) = a_{n-1}a_{n-3}\cdots a_3a_1a_2a_4\cdots a_{n-2}a_n$ if n is even, and

$A_1(\alpha_n) = a_na_{n-2}\cdots a_3a_1a_2a_4\cdots a_{n-3}a_{n-1}$ if n is odd,

and for the permutation $p(A_1, n)$ induced by A_1

$$p(A_1, n)(m) = \lceil n/2\rceil + (-1)^m\lceil (m-1)/2\rceil, \qquad 1 \leq m \leq n.$$

If m is even, then $p(A_1, n)(m) = \lceil n/2\rceil + m/2$. Then for odd n, we obtain the meaningless fixed point $m_0 = n+1$, and for even n, the trivial case $m_0 = n$ which is clear from the definition of A_1 as well. So all A_1-primes are odd.

In case m is odd, we have $p(A_1, n)(m) = \lceil n/2\rceil - (m-1)/2$ and for a possible fixed point m_0, $m_0 = \frac{2}{3}\lceil n/2\rceil + \frac{1}{3}$. Thus for n equal to $6k+1$ and $6k+2$ ($k \geq 1$), the permutation $p(A_1, n)$ possesses a fixed point.

This implies that all even numbers and the numbers $6k+1$ ($k \geq 1$) do not belong to the set of A_1-primes:

$P(A_1) = \{3, 5, 9, 11, 23, 29, 33, 35, 39, 41, 51, 53, 65, 69, 81, 83, 89, 95, 99, 105, 113,$
$119, 131, 135, 155, 173, 179, 183, 189, 191, 209, 221, \ldots\}$;

cf. sequence A163778* in [25].

Example 4.2. Again we consider the cases for α_5 and α_6. Then $A_1(\alpha_5) = a_5a_3a_1a_2a_4$, $p(A_1, 5) = (1\,3\,2\,4\,5)$, and $5 \in P(A_1)$. $A_1(\alpha_6) = a_5a_3a_1a_2a_4a_6$, $p(A_1, 6) = (1\,3\,2\,4\,5)(6)$, $\#\langle p(A_1, 6)\rangle = 5$, and $6 \notin P(A_1)$. □

Remark that with respect to their cycle structure representation we have $p(A_0, n) = p(A_0, n-1)(n)$ when n is odd, and similarly $p(A_1, n) = p(A_1, n-1)(n)$ when n is even.

Although at first sight the twist operation T has little in common with the operations A_0 and A_1, comparing $P(T)$, $P(A_0)$ and $P(A_1)$ gives rise to the following characterization.

Theorem 4.3.

(1) *A number is A_0-prime if and only if it is an even T-prime (even Queneau number).*

(2) *A number is A_1-prime if and only if it is an odd T-prime (odd Queneau number).*

Proof. First, we show that there exist a permuting operation X such that $X^{-1}T^{-1}X(\alpha_n) = A_0(\alpha_n)$ for n is even, and $X^{-1}T^{-1}X(\alpha_n) = A_1(\alpha_n)$ for n is odd. Viz. define X by $X = \rho$ and note that $\rho^{-1} = \rho$; cf. Example 1.1. Then we have for even n,

$$\begin{aligned}\rho^{-1}T^{-1}\rho(\alpha_n) &= \rho T^{-1}\rho(\alpha_n) = \rho T^{-1}(a_n a_{n-1}\cdots a_2 a_1) = \\ &= \rho(a_{n-1}a_{n-3}\cdots a_3 a_1 a_2 a_4 \cdots a_{n-2}a_n) = a_n a_{n-2}\cdots a_4 a_2 a_1 a_3 \cdots a_{n-3}a_{n-1}\end{aligned}$$

which is equal to $A_0(\alpha_n)$. Similarly, for odd n we have

$$\begin{aligned}\rho^{-1}T^{-1}\rho(\alpha_n) &= \rho T^{-1}\rho(\alpha_n) = \rho T^{-1}(a_n a_{n-1}\cdots a_2 a_1) = \\ &= \rho(a_{n-1}a_{n-3}\cdots a_4 a_2 a_1 a_3 \cdots a_{n-2}a_n) = a_n a_{n-2}\cdots a_3 a_1 a_2 a_4 \cdots a_{n-3}a_{n-1}\end{aligned}$$

which is equal to $A_1(\alpha_n)$.

The permuting operation ρ applied to the standard word α_n may be viewed as an isomorphism φ_n on Σ_n, defined by $\varphi_n(a_i) = a_{n+1-i}$ $(1 \le i \le n)$. And its inverse ρ^{-1} applied to $a_{n-1}a_{n-3}\cdots a_{n-2}a_n$ may also be considered as an isomorphism ψ_n on Σ_n, defined by

$\psi_n(a_i) = a_{i+1}$ if i is odd, and

$\psi_n(a_i) = a_{i-1}$ if i is even.

Then $\rho^{-1}T^{-1}\rho(\alpha_n) = \psi_n T^{-1}\varphi_n(\alpha_n)$. This observation implies that $P(\rho^{-1}T^{-1}\rho) = P(T^{-1})$ which in turn equals $P(T)$. Hence the statement follows from the fact that all A_0-primes are even and all A_1-primes are odd. □

When we combine Theorem 4.3 and Theorem 3.15 we obtain characterizations of A_0- and A_1-primes; cf. Theorems 4.4 and 4.5, respectively.

Theorem 4.4. *A number n in $\mathbb{N}_2$ is A_0-prime if and only if*

(1) *n is even, and*

(2) *$2n+1$ is a prime number, and*

(3) *both -2 and $+2$ are a generator of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.* □

Note that by Theorems 3.13 and 4.3, condition (1) in Theorem 4.4 may be replaced by "$n \equiv 2 \pmod 4$" as well.

Theorem 4.5. *A number n in $\mathbb{N}_2$ is A_1-prime if and only if*

(1) *n is odd, and*

(2) *$2n+1$ is a prime number, and*

(3) *only one of -2 and $+2$ is a generator of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.* □

Example 4.6. In Example 3.16(4) we showed that $6 \in P(T)$; Theorem 4.3 now implies $6 \in P(A_0)$. Similarly, from Example 3.16(3) we obtain $9 \in P(A_1)$.

But $54 \notin P(A_0)$ and $15 \notin P(A_1)$; cf. the last few (counter)examples in Section 3. □

Theorem 4.5 gives rise to the introduction of the following primes.

Definition 4.7. A number n in $\mathbb{N}_2$ is A_1^+-*prime* if it is an A_1-prime and $n \equiv 1 \pmod 4$. And n in $\mathbb{N}_2$ is an A_1^--*prime* if it is an A_1-prime and $n \equiv 3 \pmod 4$. □

For $P(A_1^+)$, we have

$$P(A_1^+) = \{5,\ 9,\ 29,\ 33,\ 41,\ 53,\ 65,\ 69,\ 81,\ 89,\ 105,\ 113,\ 173,\ 189,\ 209,\ 221,\ 233,\ 245,\ 261,\ 273,\ 281,\ 293,\ 309,\ 329,\ 393,\ 413,\ 429,\ 441,\ 453,\ 473,\ 509,\ \ldots\};$$

and for $P(A_1^-)$

$$P(A_1^-) = \{3,\ 11,\ 23,\ 35,\ 39,\ 51,\ 83,\ 95,\ 99,\ 119,\ 131,\ 135,\ 155,\ 179,\ 183,\ 191,\ 231,\ 239,\ 243,\ 251,\ 299,\ 303,\ 323,\ 359,\ 371,\ 375,\ 411,\ 419,\ 431,\ 443,\ 483,\ 491,\ \ldots\};$$

cf. sequences A163779* and A163780* in [25].

Theorems 3.15 and 4.5 imply the following characterizations of A_1^+- and A_1^--primes.

Theorem 4.8. *A number n in $\mathbb{N}_2$ is A_1^+-prime if and only if*
(1) $n \equiv 1 \pmod 4$, *and*
(2) $2n+1$ *is a prime number, and*
(3) $+2$ *is a generator of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$, but -2 is not.* □

Theorem 4.9. *A number n in $\mathbb{N}_2$ is A_1^--prime if and only if*
(1) $n \equiv 3 \pmod 4$, *and*
(2) $2n+1$ *is a prime number, and*
(3) -2 *is a generator of the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$, but $+2$ is not.* □

We return to the shuffle operations S and $\overline{S}$ of Section 2 and, particularly, to the sets $H(S)$ and $H(\overline{S})$. In Section 3 we showed that both $H(S)$ and $H(\overline{S})$ are proper subsets of $P(T)$; cf. Proposition 3.3. More precisely, by Theorems 3.3, 3.15, 4.4, 4.7 and 4.8 we have that $H(S)$ and $H(\overline{S})$ are proper subsets of $P(A_0) \cup P(A_1^+) \cup P(A_1^-) = P(T)$, where the unions are disjoint. Now we are now able to improve upon this proper inclusion.

Theorem 4.10.
(1) *A number n in $\mathbb{N}_2$ belongs to $H(S)$ if and only if n is an A_0-prime or an A_1^+-prime. Equivalently, $H(S) = P(A_0) \cup P(A_1^+)$.*
(2) *A number n in $\mathbb{N}_2$ belongs to $H(\overline{S})$ if and only if n is an A_0-prime or an A_1^--prime. Equivalently, $H(\overline{S}) = P(A_0) \cup P(A_1^-)$.*

Proof. (1) Consider an element n in $H(S)$. Then $n \geq 2$, $2n \in P(S)$, $2n+1$ is an odd prime number (Proposition 2.5), and $+2$ generates the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of the finite field $\mathbb{Z}_{2n+1}$ (Theorem 2.10). Theorems 3.15, 4.4, 4.8 and 4.9 imply that $n \in P(A_0) \cup P(A_1^+)$.

Conversely, if n belongs to $P(A_0) \cup P(A_1^+)$, then $2n+1$ is a prime number and $+2$ generates $\mathbb{Z}^\star_{2n+1}$ (Theorems 4.4 and 4.8). Then $\mathrm{ord}(2, 2n+1) = 2n$ and by Theorem 2.9 or 2.10 we have $2n \in P(S)$ and, consequently, $n \in H(S)$.

(2) The proof is similar: we use Proposition 2.14 and Theorems 2.15 and 2.15 instead of Proposition 2.5 and Theorems 2.9 and 2.10, respectively. □

Corollary 4.11. *A number n in $\mathbb{N}_2$ belongs to $H(S)$ if and only if $2n+1$ is a prime number and exactly one of the following two conditions holds:*
(1) $n \equiv 1 \pmod 4$, $+2$ *generates the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$ but -2 does not.*
(2) $n \equiv 2 \pmod 4$ *and both -2 and $+2$ generate the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

Proof. This is a consequence of Theorems 4.4, 4.8, 4.10 and the fact that $P(A_0)$ and $P(A_1^+)$ are disjoint sets. □

Corollary 4.12. *A number n in $\mathbb{N}_2$ belongs to $H(\overline{S})$ if and only if $2n+1$ is a prime number and exactly one of the following two conditions holds:*

(1) $n \equiv 2 \pmod 4$ *and both -2 and $+2$ generate the multiplicative group $\mathbb{Z}^{\star}_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

(2) $n \equiv 3 \pmod 4$, *-2 generates the multiplicative group $\mathbb{Z}^{\star}_{2n+1}$ of $\mathbb{Z}_{2n+1}$ but $+2$ does not.*

Proof. The proposition follows from Theorems 4.4, 4.9, 4.10 and the fact that $P(A_0)$ and $P(A_1^-)$ are disjoint sets. □

5 Flavius Josephus

This section is devoted to a countably infinite sequence of permuting operations on strings, denoted by $\{J_k\}_{k\geq 2}$, which are strongly related to the so-called (Flavius) Josephus' problem; cf. Section 1.3 in [12], §3.4 in [15] and [9, 21, 13]. For an excellent introduction, including many historical details, we refer to [24].

These operations are informally described as follows. For J_k, take the standard word α_n and mark the symbols at positions k, $2k$, $3k$ up to $\lfloor n/k \rfloor k$. Now concatenate the unmarked symbols to the right end of string and continue the marking process. Iterate this procedure until n symbols are marked. The final result of this permuting operation J_k is obtained by extracting the marked symbols from left to right.

Example 5.1. In order to determine $J_2(\alpha_5)$, we start marking each even position in α_5:

$a_1\overline{a_2}a_3\overline{a_4}a_5$.

Extending this string with the unmarked symbols a_1, a_3 and a_5, yields

$a_1\overline{a_2}a_3\overline{a_4}a_5a_1a_3a_5$

and further marking produces

$a_1\overline{a_2}a_3\overline{a_4}a_5\overline{a_1}a_3\overline{a_5}$.

Twice extending this string with the last unmarked symbol a_3 and marking the last occurrence of a_3, finally results in

$a_1\overline{a_2}a_3\overline{a_4}a_5\overline{a_1}a_3\overline{a_5}a_3\overline{a_3}$

from which we obtain that $J_2(\alpha_5) = a_2a_4a_1a_5a_3$. □

In the original Josephus' problem the question is to determine the last symbol to be marked. Here we use the marking procedure to define a permuting operation on strings.

It is obvious that J_1 is equal to the identity operation λ (Example 1.1), and so $P(J_1) = P(\lambda) = \varnothing$.

For the next 19 members of this family of permuting operations we have the following results with respect to their primes.

$$\begin{aligned} P(J_2) = \{&2, 5, 6, 9, 14, 18, 26, 29, 30, 33, 41, 50, 53, 65, 69, 74, 81, 86, 89, 90, 98,\\ &105, 113, 134, 146, 158, 173, 174, 186, 189, 194, 209, 210, 221, 230, 233,\\ &245, 254, 261, 270, 273, 278, 281, 293, 306, 309, 326, 329, \ldots\}, \end{aligned}$$

k	$P(J_k)$
3	3, 5, 27, 89, 1139, 1219, 1921, 2155, 5775, 9047, 12437, 78785, 105909, 197559
4	2, 5, 10, 369, 609, 1841, 2462, 3297, 3837, 14945, 94590, 98121, 965013
5	3, 15, 17, 45, 73, 83, 165, 177, 181, 229, 377, 383, 787, 2585, 3127, 3635, 4777, 36417, 63337, 166705, 418411
6	2, 13, 17, 18, 34, 49, 93, 97, 106, 225, 401, 745, 2506, 3037, 3370, 4713, 5206, 8585, 13418, 32237, 46321, 75525, 97889, 106193, 238513, 250657, 401902, 490118
7	5, 11, 21, 35, 85, 103, 161, 231, 543, 1697, 1995, 2289, 37851, 49923, 113443, 236091, 285265
8	2, 6, 10, 62, 321, 350, 686, 3217, 4981, 21785, 22305, 350878, 378446, 500241, 576033, 659057, 917342
9	3, 39, 53, 2347, 6271, 121105, 386549, 519567, 958497
10	2, 17, 98, 174, 181, 238, 6774, 9057, 44929, 54594, 58389
11	3, 9, 27, 47, 63, 185, 617, 15189, 56411, 182439, 271607, 658521
12	2, 38, 57, 145, 189, 2293, 2898, 6222, 7486, 26793, 45350, 90822, 177773
13	5, 57, 117, 187, 251, 273, 275, 665, 2511, 40393, 48615, 755921, 970037
14	2, 185, 205, 877, 2045, 3454, 6061, 29177, 928954
15	3, 9, 13, 25, 49, 361, 961, 1007, 2029, 8593, 24361, 44795, 88713
16	2, 14, 49, 333, 534, 550, 2390, 3682, 146794, 275530, 687245, 855382
17	3, 5, 7, 39, 93, 267, 557, 2389, 2467, 4059, 4681, 6213, 70507, 151013, 282477, 421135
18	2, 5, 462, 530, 6021, 14686, 19537, 67161
19	15, 145, 149, 243, 259, 449, 1921, 2787, 15871, 18563, 26459, 191515, 283269, 741343, 844805
20	2, 5, 30, 54, 81, 109, 149, 186, 513, 1089, 8158, 8533, 17178, 34478, 913274, 976402

Table 1: J_k-primes in the interval $2 \leq n \leq 1000000$ ($3 \leq k \leq 20$).

For larger values of k the results are summerized in Table 1: the search for J_k-primes for $3 \leq k \leq 20$ has been restricted to the interval $2 \leq n \leq 1000000$. This table largely extends the few numerical results mentioned at the end of Chapter 3 in [15].

The corresponding 19 sequences in [25] are A163782*, A163783*, A163784*, A163785*, A163786*, A163787*, A163788*, A163789*, A163790*, A163791*, A163792*, A163793*, A163794*, A163795*, A163796*, A163797*, A163798*, A163799*, A163800*, respectively.

Example 5.2. We already saw that $J_2(\alpha_5) = a_2a_4a_1a_5a_3$. Then $p(J_2, 5) = (1\,3\,5\,4\,2)$, and consequently 5 belongs to $P(J_2)$. It is easy to show that $J_3(\alpha_6) = a_3a_6a_4a_2a_5a_1$, $p(J_3, 6) = (1\,6\,2\,4\,3)(5)$, the order of $\langle p(J_3, 6)\rangle$ is 5, and $6 \notin P(J_3)$.

Similarly, we have for $J_2(\alpha_{14})$,

$a_1\overline{a_2}a_3\overline{a_4}a_5\overline{a_6}a_7\overline{a_8}a_9\overline{a_{10}}a_{11}\overline{a_{12}}a_{13}\overline{a_{14}}a_1\overline{a_3}a_5\overline{a_7}a_9\overline{a_{11}}a_{13}\overline{a_1}a_5\overline{a_9}a_{13}\overline{a_5}a_{13}\overline{a_{13}}$.

Consequently, $J_2(\alpha_{14}) = a_2a_4a_6a_8a_{10}a_{12}a_{14}a_3a_7a_{11}a_1a_9a_5a_{13}$, and 14 belongs to $P(J_2)$ because we have $p(J_2, 14) = (1\ 11\ 10\ 5\ 13\ 14\ 7\ 9\ 12\ 6\ 3\ 8\ 4\ 2)$. □

The remaining part of this section is restricted to the special case $k = 2$, namely, to the permutations $\{p(J_2, n)\}_{n\geq 2}$ and their properties.

In Section 3.3 of [12] an elegant method is described to solve the Josephus problem, i.e., to obtain the last symbol to be marked in the marking process. To determine the index of right-most symbol of the string $J_k(\alpha_n)$, the value of $p(J_k^{-1}, n)(n)$ has been computed in [12]. However, this approach can be extended to obtain all values of $p(J_k^{-1}, n)(m)$ for $1 \leq m \leq n$ and, in addition, to derive closed forms for both $p(J_2^{-1}, n)$ and $p(J_2, n)$. This latter achievement is rather exceptional since looking for such a closed form for $p(J_k^{-1}, n)$ or $p(J_k, n)$ with $k \geq 3$ seems to be rather difficult; cf. Section 3.3 in [12].

The idea of this method is very simple. We walk in a cyclic way through the standard word α_n of length n and we assign numbers to symbols or to symbol indices (symbol positions in α_n). In the first sweep through α_n we assign the numbers 1, 2, $\cdots$ n to the symbol positions 1, 2, $\cdots$ n, respectively.

When we restrict our attention to the special case $p(J_2, n)$, we see that the marked symbols got an even number. In the next sweep through α_n, we continue to number the symbols with an odd position in α_n: they receive the next unused numbers in the number sequence. In general, when a symbol in α_n is skipped (i.e., not marked) during the marking/numbering process, we assign a new number: the next consecutive unused number in the number sequence.

So after the first sweep we continue to number as follows: 1 becomes n+1, 2 is marked, 3 becomes n+2, 4 is marked, 5 becomes n+3, ..., $2k$+1 becomes n+k+1, $2k$+2 is marked, $2k$+3 becomes n+k+2, ..., $2n$ is marked. The jth symbol to be marked ends up with number $2j$ in this marking or numbering process.

Example 5.3. Applying this idea to $p(J_2, 14)$ yields the following scheme of indices:

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15		16		17		18		19		20		21	
22				23				24				25	
				26								27	
												28	

So 2 comes in the first place, 4 in the second, 6 in the third one, ..., 5 in the thirteenth place and, finally, 13 in the fourteenth place: $J_2(\alpha_{14}) = a_2a_4a_6a_8a_{10}a_{12}a_{14}a_3a_7a_{11}a_1a_9a_5a_{13}$; cf. Example 5.2. □

Given a final even number N in this extended marking process, we want to determine which symbol a_j arrives at position $N/2$ in the permutation $p(J_2, n)$, i.e, we want to determine the number j that satisfies $p(J_2, n)(j) = N/2$ or, equivalently, we want to compute $p(J_2^{-1}, n)(N/2)$. If $N \leq n$, then $j = N$ and a_N will be placed at position $N/2$. However, if $N > n$, the marking number N should have a (smaller) predecessor, which in turn may possess a (smaller) predecessor, etc. But after a finite number of iterations we end up with a symbol index j in between 1 and n.

In Section 3.3 of [12] this iteration process is captured in an algorithm to determine the value of $p(J_3^{-1}, n)(n)$. This algorithm can easily be generalized —viz. to compute all values $p(J_3^{-1}, n)(m)$ of the permutation— and simplified, since starting with J_2 instead of J_3 means a considerable reduction in structural complexity. The resulting, modified algorithm for computing $p(J_2^{-1}, n)(m)$ with $1 \leq m \leq n$, reads as follows.

$N := 2 * m;$
while $N > n$ **do** $N := 2 * (N - n) - 1;$
$p(J_2^{-1}, n)(m) := N.$

As in Section 3.3 of [12] we transform the above algorithm in an even simpler one:

$D := 2 * n + 1 - 2 * m;$
while $D \leq n$ **do** $D := 2 * D;$
$p(J_2^{-1}, n)(m) := 2 * n + 1 - D.$

Example 5.4. Applying these algorithms with $n = 14$ and $m = 4$ results, after skipping the loops, in $p(J_2^{-1}, 14)(4) = 8$. When we start the first algorithm with $m = 14$, the successive values of N are 28, 27, 25, 21 and 13; thus $p(J_2^{-1}, 14)(14) = 13$; the second algorithm yields for D the values: 1, 2, 4, 8 and 16. For $m = 13$, the second algorithm gives 3, 6, 12 and 24 as D-values, which implies $p(J_2^{-1}, 14)(13) = 5$; cf. Example 5.3. □

Let $L(m, n)$ denote the number of times the loop in this latter algorithm has been executed. After leaving the loop we have

$(2n + 1 - 2m) \cdot 2^{L(m,n)} \geq n + 1$

which yields

$L(m, n) = \lceil \lg \frac{n+1}{2n+1-2m} \rceil$

where we use "lg" to denote the base-2 or binary logarithm as in [12]. Consequently,

$$p(J_2^{-1}, n)(m) = 2m \qquad \text{if } 1 \leq m < k = \lceil (n+1)/2 \rceil, \text{ and}$$
$$p(J_2^{-1}, n)(m) = 2n + 1 - (2n+1-2m)2^{\lceil \lg \frac{n+1}{2n+1-2m} \rceil} \qquad \text{if } k \leq m \leq n.$$

This definition of $p(J_2^{-1}, n)$ is equivalent to

$$p(J_2^{-1}, n)(m) \equiv +2m \pmod{2n+1} \qquad \text{if } 1 \leq m < k = \lceil (n+1)/2 \rceil, \text{ and}$$
$$p(J_2^{-1}, n)(m) \equiv +2m \cdot 2^{\lceil \lg \frac{n+1}{2n+1-2m} \rceil} \pmod{2n+1} \qquad \text{if } k \leq m \leq n,$$

which can even be reduced to the closed form

$$p(J_2^{-1},n)(m) \equiv +2m \cdot 2^{\lceil \lg \frac{n+1}{2n+1-2m} \rceil} \pmod{2n+1} \qquad 1 \le m \le n,$$

or even to

$$p(J_2^{-1},n)(m) \equiv +2m \cdot \llbracket \tfrac{n+1}{2n+1-2m} \rrbracket \pmod{2n+1} \qquad 1 \le m \le n,$$

where $\llbracket x \rrbracket$ denotes the smallest value 2^t with $t \in \mathbb{N}$ such that $x \le 2^t$.

For even m, it is now easy to define $p(J_2,n)$: $p(J_2,n)(m) = m/2$ if m is even. But for odd values of m, the situation is not that straightforward. There does not seem to be an easy way to invert the various definitions of $p(J_2^{-1},n)$.

Fortunately, there is a way out: we can "invert" our two algorithms, which results in

$N := m;$
while N is odd **do** $N := (2*n+1+N)/2;$
$p(J_2,n)(m) := N/2$

and, respectively,

$D := 2*n+1-m;$
while D is even **do** $D := D/2;$
$p(J_2,n)(m) := (2*n+1-D)/2.$

Example 5.5. If we execute these algorithms with $n = 14$ and $m = 8$, the loops will be skipped, and $p(J_2,14)(8) = 4$. For $m = 13$, the first algorithm yields 13, 21, 25, 27 and 28 as successive values of N; so $p(J_2,14)(13) = 14$. The second algorithm obtains the D-values: 16, 8, 4, 2 and 1; hence $p(J_2,14)(13) = 14$; cf. Example 5.4. □

From the second algorithm we derive that

$$p(J_2,n)(m) = (2n+1-\lfloor\!\lfloor 2n+1-m \rfloor\!\rfloor)/2 \qquad (1 \le m \le n),$$

where $\lfloor\!\lfloor x \rfloor\!\rfloor$ is the odd number such that $x/\lfloor\!\lfloor x \rfloor\!\rfloor$ is a power of 2. For instance, we have $\lfloor\!\lfloor 16 \rfloor\!\rfloor = 1$, $\lfloor\!\lfloor 24 \rfloor\!\rfloor = 3$ and $\lfloor\!\lfloor 120 \rfloor\!\rfloor = 15$.

The following auxiliary result happens to be useful and it is of some interest of its own.

Lemma 5.6. *For each integer n with $n \ge 1$,*

$$\sum_{m=1}^{n} \left\lceil \lg \frac{n+1}{2m-1} \right\rceil = n.$$

Proof. Our argument is based on Exercise 3.34 in [12]. Let s_n denote this sum. Then

$$s_n = \sum_{m=1}^{n} \left\lceil \lg \frac{n+1}{2m-1} \right\rceil = \sum_{m=1}^{\lceil n/2 \rceil} \left\lceil \lg \frac{n+1}{2m-1} \right\rceil,$$

since for $m > \lceil n/2 \rceil$, each term $\lceil \lg \frac{n+1}{2m-1} \rceil$ vanishes. Let $k = \lceil \lg \lceil n/2 \rceil \rceil$. Then $2^k \le n-1$ and equality only happens when $n = 2^t + 1$ for some t in $\mathbb{N}$.

To the sum s_n we add $2^k - \lceil n/2 \rceil$ terms equal to 0 to simplify the calculations at the boundary. In other words, we extend the summation to 2^k terms instead of n or $\lceil n/2 \rceil$.

In the following derivation we used Iverson's convention: the expression "$(\,P(x)\,)$" evaluates to 1 if the predicate $P(x)$ is true and to 0 if $P(x)$ is false[12]. For instance, $\sum_{m=1}^{n} a_m$ may be written as $\sum a_m(1 \le m \le n)$ using this convention.

Then we have

$$\begin{aligned}
s_n &= \sum_{m=1}^{2^k} \left\lceil \lg \frac{n+1}{2m-1} \right\rceil \;=\; \sum_{j,m} j \;\left(j = \left\lceil \lg \frac{n+1}{2m-1} \right\rceil \right) \;(1 \le m \le 2^k) \\
&= \sum_{j,m} j \;\left(2^{j-1} < \frac{n+1}{2m-1} \le 2^j \right) \;(1 \le j \le \lceil \lg(n+1) \rceil) \\
&= \sum_{j,m} j \;\left(\frac{n+1+2^j}{2^{j+1}} \le m < \frac{n+1+2^{j-1}}{2^j} \right) \;(1 \le j \le \lceil \lg(n+1) \rceil) \\
&= \sum_{j,m} j \;\left(m \in \left[\frac{n+1+2^j}{2^{j+1}}, \frac{n+1+2^{j-1}}{2^j} \right) \right) \;(1 \le j \le \lceil \lg(n+1) \rceil) \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} j \;\left(\left\lceil \frac{n+1+2^{j-1}}{2^j} \right\rceil - \left\lceil \frac{n+1+2^j}{2^{j+1}} \right\rceil \right) \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} j \;\left(\left\lceil \frac{2n+2+2^j}{2^{j+1}} \right\rceil - \left\lceil \frac{n+1+2^j}{2^{j+1}} \right\rceil \right) \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} \left\lceil \frac{2n+2+2^j}{2^{j+1}} \right\rceil - \lceil \lg(n+1) \rceil \cdot \left\lceil \frac{n+1+2^{\lceil \lg(n+1) \rceil}}{2^{\lceil \lg(n+1) \rceil + 1}} \right\rceil \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} \left\lceil \frac{n+1}{2^j} + \frac{1}{2} \right\rceil - \lceil \lg(n+1) \rceil \;=\; \sum_{j=1}^{\lceil \lg(n+1) \rceil} \left\lceil \frac{n+1}{2^j} - \frac{1}{2} \right\rceil .
\end{aligned}$$

In the fifth line of this derivation we used the fact that the interval $[\alpha, \beta)$ contains exactly $\lceil \beta \rceil - \lceil \alpha \rceil$ integers. The seventh line has been obtained by "telescoping" [12], and the last line is the result of using $\lceil x \rceil = \lceil x - 1 \rceil + 1$.

Next we consider the sums s_{n-1} and s_n: for all but one value of j the jth terms in these sums are equal, i.e.,

$$\left\lceil \frac{n+1}{2^j} - \frac{1}{2} \right\rceil = \left\lceil \frac{(n-1)+1}{2^j} - \frac{1}{2} \right\rceil ;$$

cf. Exercise 3.22 in [12]. The only exception is when $j = 1 + \lg(n/\lVert n \rVert)$ where $\lVert n \rVert$ is again the odd integer such that $n/\lVert n \rVert$ is a power of 2. In this exceptional case we have

$$\left\lceil \frac{n+1}{2^j} - \frac{1}{2} \right\rceil = 1 + \left\lceil \frac{(n-1)+1}{2^j} - \frac{1}{2} \right\rceil ,$$

which implies that $s_n = s_{n-1} + 1$. Together with $s_1 = 1$ this yields $s_n = n$. □

The proof of this lemma is completely according to the style of [12], but it is a bit complicated. There is, however, an alternative proof, based on a combinatorial argument of a staggering simplicity.

Alternative proof of Lemma 5.6. We first observe that for each n with $n \geq 1$, we have

$$s_n = \sum_{m=1}^{n} \left\lceil \lg \frac{n+1}{2m-1} \right\rceil = \sum_{m=1}^{n} \left\lceil \lg \frac{n+1}{2n+1-2m} \right\rceil = \sum_{m=1}^{n} L(m,n) = C(2n,n)$$

where $L(m,n)$ is the number of times the loop has been executed in either of our algorithms to compute $p(J_2^{-1},n)$ on input m.

The entity $C(2n,n)$ is related to the following very simple combinatorial problem.

> Given m points, we construct n ($n \leq m$) chains (linear orders, or monadic trees) of length greater than or equal to 0. What is the total length $C(m,n)$ (i.e., the total number of edges) of these n chains?

To construct the n chains we need n points for n roots. The remaining points will be used for edges: each point yields an additional edge. Therefore $C(m,n) = m - n$.

To determine s_n, we return to our marking/numbering process: we have $2n$ points to build n chains; so $s_n = C(2n,n) = 2n - n = n$.

Notice that the way in which we achieve these n chains is immaterial; any set of n chains based on $2n$ points has total length n. The observation that our marking/numbering procedure (cf. Example 5.3) is just one particular instance of "n chains based on $2n$ points" completes the proof. □

Example 5.7. Returning to Example 5.3, we have 28 points and we use the points 1, 2, ... , 14 for the roots of the 14 chains; the chains with the even numbered roots have length 0. Chains rooted with 3, 7 and 11 have length 1, those rooted with 1 and 9 have length 2. The remaining chains have length 3 (root 5) and 4 (root 13); hence $C(28,14) = 14$. □

In the context of the present paper, the use of $p(J_2^{-1},n)$ is much more convenient than applying $p(J_2,n)$. Therefore we will state our results in terms of J_2, but in proofs we will frequently use J_2^{-1}. In other words, we will heavely rely on the equality $P(J_2) = P(J_2^{-1})$, i.e., a number is a J_2-prime if and only if it is a J_2^{-1}-prime. Typical applications of this convention are (the proofs of) Proposition 5.8, Lemma 5.9, Proposition 5.10 and their consequences.

For J_2 we also have a result similar to Propositions 2.2(1) and 3.4:

Proposition 5.8. *If n in $\mathbb{N}_2$ is J_2-prime, then for each m ($1 \leq m < 2n+1$):*

(1) *If $n \equiv 1 \pmod 4$, then $m \cdot 2^n \equiv -m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv +m \pmod{2n+1}$.*

(2) *If $n \equiv 2 \pmod 4$, then $m \cdot 2^n \equiv -m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv -m \pmod{2n+1}$.*

Proof. We apply the permutation $p(J_2^{-1},n)$ iteratively n times to m: this results in all values 1, 2, ... , n in some order and $p^n(J_2^{-1},n)(m) = m$, as n is J_2^{-1}-prime. Using Lemma 5.6, we obtain

$$\begin{aligned} p^n(J_2^{-1},n)(m) &\equiv 2^n \cdot m \cdot \textstyle\prod_{j=1}^{n} 2^{\lceil \lg \frac{n+1}{2n+1-2j} \rceil} && (\mathrm{mod}\ 2n{+}1)\\ &\equiv 2^n \cdot m \cdot 2^{\sum_{j=1}^{n} \lceil \lg \frac{n+1}{2n+1-2j} \rceil} && (\mathrm{mod}\ 2n{+}1)\\ &\equiv 2^n \cdot m \cdot 2^{\sum_{j=1}^{n} \lceil \lg \frac{n+1}{2j-1} \rceil} && (\mathrm{mod}\ 2n{+}1)\\ &\equiv m \cdot 2^{2n} && (\mathrm{mod}\ 2n{+}1). \end{aligned}$$

This implies $m \cdot 2^{2n} \equiv m \,(\mathrm{mod}\ 2n{+}1)$ and $2^{2n} \equiv 1 \,(\mathrm{mod}\ 2n{+}1)$. By an argument almost identical to the one we used in proving Proposition 2.2(1) —except that we use $2n$ instead of n— we obtain that $m \cdot 2^n \equiv -m \,(\mathrm{mod}\ 2n{+}1)$.

If $n = 4k{+}1$ $(k \geq 1)$, then $m \cdot (-2)^n \equiv m \cdot 2^n(-1)^{4k+1} \equiv +m \,(\mathrm{mod}\ 2n{+}1)$, and if $n = 4k{+}2$ $(k \geq 0)$, we get $m \cdot (-2)^n \equiv -m \,(\mathrm{mod}\ 2n{+}1)$. □

In Proposition 5.8 the cases $n \equiv 0 \,(\mathrm{mod}\ 4)$ and $n \equiv 3 \,(\mathrm{mod}\ 4)$ are not included because whenever n satisfies either of these conditions, n is not J_2-prime; cf. Theorem 5.11 below.

The first definition of $p(J_2^{-1}, n)$ enables us to establish J_2-counterparts of Lemma 3.7 and Proposition 3.8.

Lemma 5.9. *If there exist integers x and y with $x, y \geq 1$ such that $n = 2xy + x + y$, then n is not J_2-prime.*

Proof. We just need to modify the proof of Lemma 3.7 slightly: we only need to show that $p(J_2^{-1}, n)$ also maps every multiple of $2x + 1$ on another multiple of $2x + 1$. For multiples $m(2x + 1)$ with $1 \leq m(2x + 1) < \lceil (n + 1)/2 \rceil$ this is evident and for multiples $m(2x + 1)$ with $\lceil (n + 1)/2 \rceil \leq m(2x + 1) \leq n$, we have

$$\begin{aligned} p(J_2^{-1},n)(m(2x+1)) &= 2n+1-(2n+1-2m(2x+1))E\\ &= 2(2xy+x+y)+1-(2(2xy+x+y)+1-2m(2x+1))E\\ &= 4xy+2y+2x+1-(4xy+2y+2x+1-4mx-2m)E\\ &= (2x+1)(2y+1-(2y+1-2m)E), \end{aligned}$$

where E stands for $2^{\lceil \lg \frac{n+1}{2n+1-2m(2x+1)} \rceil}$. □

Proposition 5.10. *If n is J_2-prime, then $2n + 1$ is a prime number.*

Proof. The argument is identical to the proof of Proposition 3.8 except that we use Lemma 5.9 instead of Lemma 3.7. □

Theorem 5.11. *Let n be a number in $\mathbb{N}_2$. If $n \equiv 0 \,(\mathrm{mod}\ 4)$ or $n \equiv 3 \,(\mathrm{mod}\ 4)$, then n is not J_2-prime.*

Proof. In both cases the arguments are very similar to the one of Theorem 3.13.

The assumption that n, with $n = 4k$ $(k \geq 1)$ is J_2-prime, implies that $2n{+}1 = 8k{+}1$ is a prime number p (Proposition 5.10) and that $+2$ is quadratic residue of p (Proposition 3.10). In the very same way, we obtain that $+2$ is quadratic residue of $p = 8k + 7$ when we assume that $n = 4k + 3$ $(k \geq 0)$ is J_2-prime.

Now it is straightforward to derive a contradiction; cf. the proof of Theorem 3.13. □

We now turn to the main result of this section.

Theorem 5.12. *A number n is J_2-prime if and only if $2n+1$ is a prime number and exactly one of the following two conditions holds:*

(1) $n \equiv 1 \pmod 4$ *and $+2$ generates the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$ but -2 does not.*

(2) $n \equiv 2 \pmod 4$ *and both -2 and $+2$ generate the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

Proof. Using Propositions 5.8 and 5.10 (instead of Proposition 3.4 and 3.8) and Theorem 5.11 (instead of Theorem 3.13) the proof is analogous to the one of Theorem 3.15. □

Example 5.13. (1) The number 21 is not J_2-prime. Though $21 \equiv 1 \pmod 4$ and 43 is a prime number, both $+2$ and -2 fail to generate the multiplicative group $\mathbb{Z}^\star_{43}$ of $\mathbb{Z}_{43}$. The set of possible generators of this group is $\{-17, -15, -14, -13, -10, -9, 3, 5, 12, 18, 19, 20\}$.
(2) For $n = 9$, we have $9 \equiv 1 \pmod 4$, 19 is prime, $+2$ generates $\mathbb{Z}^\star_{19}$ but -2 does not, and $9 \in P(J_2)$; cf. Example 3.16(3).
(3) When $n = 6$, we obtain $6 \equiv 2 \pmod 4$, 13 is prime, both $+2$ and -2 generate $\mathbb{Z}^\star_{13}$, and so 6 is J_2-prime; cf. Example 3.16(4). □

The characterization of J_2-primes in Theorem 5.12 can, of course, be related to the main resluts of Section 4.

Theorem 5.14. *A number n is J_2-prime if and only if either n is A_0-prime or n is A_1^+-prime: $P(J_2) = P(A_0) \cup P(A_1^+)$. Equivalently, a number n is J_2-prime if and only if $2n+1$ is a prime number and $+2$ generates the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

Proof. Theorems 4.4, 4.8 and 5.12. □

Corollary 5.15. $P(J_2) = H(S)$.

Proof. Theorems 4.10(1) and 5.14. □

6 Duality

In Section 2 we introduced a permuting operation $\overline{S}$ on strings to which we referred as the dual of the permuting operation S without giving a formal definition of duality. In the previous sections we have met a number of permuting operations and the characterizations of the corresponding primes which makes it easier to propose such a formal definition.

Definition 6.1. Let X be permuting operation on strings of which $P(X)$ can be characterized as: "a number n in $\mathbb{N}_2$ is X-prime if and only if $\gamma(n)$ is a prime number and exactly one of the following K conditions holds ($1 \le i \le K$):

(*i*) $P_i(n)$ and $g_{i,1}, \ldots, g_{i,M(i)}$ ($M(i) \ge 1$) generate the multiplicative group $\mathbb{Z}^\star_{\gamma(n)}$ of $\mathbb{Z}_{\gamma(n)}$ but $h_{i,1}, \ldots, h_{i,N(i)}$ ($N(i) \ge 0$) do not",

where $\gamma : \mathbb{N} \to \mathbb{N}$ is a function that increases monotonically in n, and the P_i's are mutually exclusive predicates, i.e., for given n, at most one of the P_i's ($1 \le i \le K$) is true.

A permuting operation on strings Y is called *dual* to X, if $P(Y)$ can be characterized as: "a number n in $\mathbb{N}_2$ is Y-prime if and only if $\gamma(n)$ is a prime number and exactly one of the following K conditions holds ($1 \leq i \leq K$):

(i) $Q_i(n)$ and $-g_{i,1}, \ldots, -g_{i,M(i)}$ ($M(i) \geq 1$) generate the multiplicative group $\mathbb{Z}^{\star}_{\gamma(n)}$ of $\mathbb{Z}_{\gamma(n)}$ but $-h_{i,1}, \ldots, -h_{i,N(i)}$ ($N(i) \geq 0$) do not",

where the Q_i's are mutually exclusive predicates, and there exists a bijection (i.e., an injective and surjective mapping)

$$\varphi : \{P_i \mid 1 \leq i \leq K\} \to \{Q_i \mid 1 \leq i \leq K\}.$$

If Y is dual to X and $Y = X$, then we call the permuting operation X *self-dual*. □

Example 6.2. (1) The permuting operation $\overline{S}$ is indeed dual to S: $K = 1$, $\gamma(n) = n{+}1$, $M(1) = 1$, $N(1) = 0$ and $g_{1,1} = +2$; cf. Theorems 2.10 and 2.16. On the other hand S is dual to $\overline{S}$ as well.

(2) According to Theorems 4.8 and 4.9, the permuting operation A_1^- is dual to A_1^+: $K = 1$, $\gamma(n) = 2n{+}1$, $M(1) = 1$, $N(1) = 1$, $g_{1,1} = +2$, $h_{1,1} = -2$, $P_1(n)$ is "$n \equiv 1 \pmod 4$", $Q_1(n)$ is "$n \equiv 3 \pmod 4$", and $\varphi(P_1) = Q_1$.

(3) The permuting operations T, A_0 and A_1 are self-dual. □

Definition 6.1 suggests, like many similar definitions, two quite general problems:

Existence problem: Given a permuting operation X, does there exists a permuting operation $\overline{X}$ that is dual to X?

Unicity problem: Given permuting operations X and $\overline{X}$ such that $\overline{X}$ is dual to X, is $\overline{X}$ unique?

Remark that for each permuting operation considered so far, with the exception of J_2, we have solved the existence problem[5].

With respect to the unicity problem, the answer is probably negative in general. Although T is dual to T, we will propose a dual $\overline{T}$ of T which is unequal to T.

Simply defining a candidate dual $p(T_c, n)$ of $p(T, n)$ by

$$\begin{aligned} p(T_c,n)(m) &\equiv -2m - n \pmod{2n{+}1} && \text{if } 1 \leq m < k = \lceil (n+1)/2 \rceil, \text{ and} \\ p(T_c,n)(m) &\equiv +2m - n \pmod{2n{+}1} && \text{if } k \leq m \leq n \end{aligned}$$

will not work as $p(T_c, n)(n) = n$ for each $n \in \mathbb{N}_2$ and hence $P(T_c) = \varnothing$. More promising is $p(\overline{T}, n)$ defined by

$$\begin{aligned} p(\overline{T},n)(m) &= n + 2 - 2m && \text{if } 1 \leq m \leq k = \lceil n/2 \rceil, \text{ and} \\ p(\overline{T},n)(m) &= 2(m-k) - d && \text{if } k < m \leq n; \end{aligned}$$

where $d = 1$ if n is even and $d = 0$ if n is odd.

[5]We exclude the permuting operations J_k for $k \geq 3$ from our study of duality because of the complete lack of characterization resluts for $P(J_k)$ with $k \geq 3$. According to Definition 6.1 such characterizations are a prerequisite for duality.

Computing the first few elements of the set of $\overline{T}$-primes shows that $P(\overline{T})$ is probably equal to $P(T)$. This is also confirmed by the distribution of $\overline{T}$-primes, a subject discussed in the next section. We leave it as an exercise to the interested reader to show that

(i) $P(\overline{T}) = P(T)$, and

(ii) $P(\overline{T})$ possesses a characterization as Theorem 3.15.

We now return to the existence problem and, in particular, to the instance that has left open: viz. the quest for a dual $\overline{J_2}$ for J_2. Unfortunately, J_2 itself does not give rise to some straightforward proposal for $\overline{J_2}$, but when we start with J_2^{-1} there is a way out.

Remember that $p(J_2^{-1}, n)(m) \equiv +2m \pmod{2n+1}$ if $1 \leq m < k = \lceil (n+1)/2 \rceil$; cf. Section 5. For $\overline{J_2}^{-1}$ we define

$$p(\overline{J_2}^{-1}, n)(m) \equiv -2m \pmod{2n+1} \qquad \text{if } k \leq m \leq n,$$

which yields the odd integers in between 1 and n in reversed order when m increases from k to n. The even integers are obtained in a more complicated way which can be explained better in the way J_2 is described in Section 3.3 of [12]; cf. Section 5.

We will number the symbol positions in the standard word α_n as in Section 5, but we will distinguish between even numbered and odd numbered sweeps through α_n:

• In odd numbered sweeps we number from left to right downwards starting with $2n$ in the first sweep.

• In even numbered sweeps we number from left to right upwards starting with 1 in the second sweep.

• The numbering ends when all numbers from 1 to $2n$ are assigned to symbol positions.

Alternating between odd and even numbered sweeps shows the effect of the minus sign. As in Section 3.3 of [12] the even numbers in the numbering/marking process determine the value of $p(\overline{J_2}, n)(m)$: the jth symbol to be marked receives number $2j$ in the marking process.

This numbering/marking process will become more clear when we consider a concrete example.

Example 6.3. We apply this numbering process to $p(\overline{J_2}, 14)$. As in Section 5 we consider indices of symbols (symbol position) in the standard word α_{14} rather than the symbols themselves. In the following scheme each sweep is preceded by its sweep number s as (s):

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
(1)	28	27	26	25	24	23	22	21	20	19	18	17	16	15
(2)		1		2		3		4		5		6		7
(3)		14				13				12				11
(4)						8								9
(5)														10

From this scheme we infer that $\overline{J_2}^{-1}(\alpha_{14}) = a_{14}a_7a_{13}a_1a_{12}a_6a_{11}a_2a_{10}a_6a_9a_3a_8a_5$ and, consequently, that $\overline{J_2}(\alpha_{14}) = a_4a_8a_{12}a_6a_{14}a_{10}a_2a_{13}a_{11}a_9a_7a_5a_3a_1$. Therefore $p(\overline{J_2}, 14) =$ (1 4 6 10 9 11 7 2 8 13 3 12 5 14), $\#\langle p(\overline{J_2}, 14)\rangle = 14$ and $14 \in P(\overline{J_2})$. □

As in Section 5 we want to determine the value of $p(\overline{J_2}^{-1}, n)(N/2)$ given N. For $N > n$, this is trivial, since $p(\overline{J_2}^{-1}, n)(N/2) = 2n{+}1{-}N$. But if $N \leq n$, N has a predecessor, which in turn may also possess a predecessor, etc. As for $p(J_2^{-1}, n)$ there are simple algorithms to compute $p(\overline{J_2}^{-1}, n)$:

$N := 2 * m;$

while $N \leq n$ **do** $N := 2 * n + 1 - 2 * N;$

$p(\overline{J_2}^{-1}, n)(m) := 2 * n + 1 - N$

and, respectively,

$D := 2 * n + 1 - 2 * m;$

while $D > n$ **do** $D := (-2 * D) \bmod (2 * n + 1);$

$p(\overline{J_2}^{-1}, n)(m) := D.$

In this latter algorithm the binary mod-operation is used; it should not be confused with the congruence relation $a \equiv b \pmod{p}$.

Example 6.4. When we apply these algorithms with $n = 14$ and $m = 11$, then $N = 22$ and $D = 7$, the loops will be skipped and $p(\overline{J_2}^{-1}, 14)(11) = 7$. Starting the first algorithm with $m = 5$, yields as successive values of N: 10, 9, 11, 7 and 15; hence $p(\overline{J_2}^{-1}, 14)(5) = 14$. For $m = 5$, the second algorithm obtains as successive D-values: 19, 20, 18, 22 and 14 and it results in $p(\overline{J_2}^{-1}, 14)(5) = 14$ as well; cf. Example 6.3. □

To derive a mathematical expression for $p(\overline{J_2}^{-1}, n)$ from these algorithms is not as straightforward as in the case of $p(J_2^{-1}, n)$.

When we want to proceed as in Section 5, we encounter two complications, the first of which is easy to deal with, but the second one is more involved.

First of all, we have to exclude the case $n \equiv 1 \pmod 3$, but this happens to be no serious restriction. When $\overline{J_2}$ turns out to be a dual of J_2 we know that for each $\overline{J_2}$-prime or, equivalently, for each $\overline{J_2}^{-1}$-prime n, the number $2n{+}1$ is a prime number. But if $n \in \mathbb{N}_2$ satisfies $n \equiv 1 \pmod 3$, then $2n{+}1$ is divisible by 3. Consequently, no $n \in \mathbb{N}_2$ with $n \equiv 1 \pmod 3$ is $\overline{J_2}$-prime.

This excluded case corresponds to the phenomenon that the last number assigned in the numbering or marking process is odd instead of even.

Example 6.5. Applying the marking/numbering process to $p(\overline{J_2}, 13)$ yields the following scheme.

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

Notice that $13 \equiv 1 \pmod 3$ and that 10 is assigned in sweep (5) before 9 in sweep (6). □

Secondly, we have to distinguish between an odd and an even number of times that the loop has been executed in these algorithms. Let $L(m, n)$ denote the number of times that the loop has been executed in any of these two algorithms when the input is m. Then $L(m, n)$ is odd when $1 \leq m \leq u = \lfloor n/3 \rfloor$, and $L(m, n)$ is even when $u < m \leq n$.

Example 6.6. We return to the case $n = 14$; cf. Example 6.3. For $L(m, n)$ we have the following values:

$p(\overline{J_2}, 14)(m)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(m, n)$	0	2	0	1	0	3	0	1	0	2	0	1	0	4
m	14	7	13	1	12	4	11	2	10	6	9	3	8	5

Now for $n = 14$, we have $u = 4$, $L(m, n)$ is odd when $1 \leq m \leq 4$, whereas $L(m, n)$ is even when $4 < m \leq 14$. □

Let N_i $(i \geq 0)$ denote the value of N in the first algorithm when the loop has been visited i times. So $N_0 = 2m$ and

$N_1 = p - 4m$	$N_2 = 8m - p$
$N_3 = 3p - 16m$	$N_4 = 32m - 5p$
$N_5 = 11p - 64m$	$N_6 = 128m - 21p$
$N_7 = 43p - 256m$	$N_8 = 512m - 85p$
$N_9 = 171p - 1024m$	$N_{10} = 2048m - 341p$

where $p = 2n+1$. From these first few values of N_i $(i \geq 0)$, it is easy to infer that for $t \geq 0$, we have:

$N_{2t+1} = (2 \cdot 4^t + 1)p/3 - 4^{t+1} \cdot m$, and

$N_{2t} = 2 \cdot 4^t \cdot m - (4^t - 1)p/3$.

From these expressions it easily follows that $N_{i+2} - N_{i+1} = -2(N_{i+1} - N_i)$ or, in other words, N_i is the solution of the difference equation

$N_{i+2} + N_{i+1} - 2N_i = 0$

with initial values $N_0 = 2m$ and $N_1 = 2n + 1 - 4m$. Solving this equation yields

$N_i = ((6m - 2n - 1)(-2)^i + 2n + 1)/3 = 2m \cdot (-2)^i + (2n + 1)(1 - (-2)^i)/3$.

Since $(1-(-2)^i)/3$ is an integer, we have for each $i \geq 0$ that $N_i \equiv 2m\cdot(-2)^i \pmod{2n+1}$ provided that $n \not\equiv 1 \pmod 3$.

Knowing N_i we are able to determine $L(m, n)$. Again we distinguish two cases:

Case 1: i is odd and $1 \leq m \leq u = \lfloor n/3 \rfloor$. After the last visit of the loop we have

$N_i = ((6m - 2n - 1)(-2)^i + 2n + 1)/3 < 2n + 1$, or

$-2^i < (6n + 3 - 2n - 1)/(6m - 2n - 1) = (4n + 2)/(6m - 2n - 1)$, i.e.,

$2^i > (4n + 2)/(2n + 1 - 6m)$, and so

$L(m, n) = \left\lfloor \lg \frac{4n+2}{2n+1-6m} \right\rfloor_O$ with $1 \leq m \leq \lfloor n/3 \rfloor$,

where $\lfloor x \rfloor_O$ is the largest odd integer smaller than or equal to x.

Case 2: i is even and $u < m < k = \lceil (n + 1)/2 \rceil$. After leaving the loop we have

$N_i = ((6m - 2n - 1)(-2)^i + 2n + 1)/3 \geq n + 1$, but now

$2^i \geq (n + 2)/(6m - 2n - 1)$, and therefore

$L(m, n) = \left\lceil \lg \frac{n+2}{6m-2n-1} \right\rceil_E$ with $\lfloor n/3 \rfloor < m < k = \lceil (n + 1)/2 \rceil$,

where $\lceil x \rceil_E$ is the smallest even integer greater than or equal to x.

For $p(\overline{J_2}^{-1}, n)$ we now obtain the following definition in case $n \not\equiv 1 \pmod 3$.

$p(\overline{J_2}^{-1}, n)(m) \equiv +2m \cdot 2^{\left\lfloor \lg \frac{4n+2}{2n+1-6m} \right\rfloor_O} \pmod{2n+1}$ if $1 \leq m \leq u = \lfloor n/3 \rfloor$, and

$p(\overline{J_2}^{-1}, n)(m) \equiv -2m \cdot 2^{\left\lceil \lg \frac{n+2}{6m-2n-1} \right\rceil_E} \pmod{2n+1}$ if $u < m < k = \lceil (n+1)/2 \rceil$.

$p(\overline{J_2}^{-1}, n)(m) \equiv -2m \pmod{2n+1}$ if $k \leq m \leq n$.

As $\left\lceil \lg \frac{n+2}{6m-2n-1} \right\rceil_E = 0$ for $k \leq m \leq n$, we have when $n \not\equiv 1 \pmod 3$:

$p(\overline{J_2}^{-1}, n)(m) \equiv +2m \cdot 2^{\left\lfloor \lg \frac{4n+2}{2n+1-6m} \right\rfloor_O} \pmod{2n+1}$ if $1 \leq m \leq u = \lfloor n/3 \rfloor$,

$p(\overline{J_2}^{-1}, n)(m) \equiv -2m \cdot 2^{\left\lceil \lg \frac{n+2}{6m-2n-1} \right\rceil_E} \pmod{2n+1}$ if $u < m \leq n$.

The $\lfloor x \rfloor_O$ and $\lceil x \rceil_E$ in this definition may be removed by using the following equalities:

$\lceil x \rceil_E = 2 \cdot \lceil x/2 \rceil$, $\lceil x \rceil_O = 2 \cdot \lceil (x - 1)/2 \rceil + 1$,

$\lfloor x \rfloor_E = 2 \cdot \lfloor x/2 \rfloor$, $\lfloor x \rfloor_O = 2 \cdot \lfloor (x - 1)/2 \rfloor + 1$,

which also imply that $\lceil x \rceil_O = \lceil x - 1 \rceil_E + 1$ and $\lfloor x \rfloor_O = \lfloor x - 1 \rfloor_E + 1$.

Example 6.7. First, we consider the case $n = 14$, i.e., $p(\overline{J_2}^{-1}, 14)$; so let $u = \lfloor n/3 \rfloor = 4$, $k = \lceil (n+1)/2 \rceil = 7$, $L(m, 14) = \lfloor \lg(58/(29-6m)) \rfloor_O$ if $1 \leq m \leq 4$ and $L(m, 14) = \lceil \lg(16/(6m - 29)) \rceil_E$ if $4 < m \leq 14$.

m	1	2	3	4	5	6	7	8	9	$10 \le m \le 14$
$L(m,14)$	1	1	1	3	4	2	2	0	0	0
$+2m \cdot 2^{L(m,14)}$	4	8	12	64	—	—	—	—	—	—
$-2m \cdot 2^{L(m,14)}$	—	—	—	—	-160	-48	-56	-16	-18	$-2m$
$p(\overline{J_2}^{-1},14)(m)$	4	8	12	6	14	10	2	13	11	$29-2m$

In Example 6.3 we determined $\overline{J_2}^{-1}(\alpha_{14})$ from which it is easy to infer that $p(\overline{J_2}^{-1},14) =$ (1 14 5 12 3 13 8 2 7 11 9 10 6 4). This agrees with the last line in this table.

Similarly, for $n = 17$, i.e. for $p(\overline{J_2}^{-1},17)$, we have $u = \lfloor n/3 \rfloor = 5$, $k = \lceil (n+1)/2 \rceil = 9$, $L(m,17) = \lfloor \lg(70/(35-6m)) \rfloor_O$ if $1 \le m \le 5$ and $L(m,17) = \lceil \lg(19/(6m-35)) \rceil_E$ if $5 < m \le 17$.

m	1	2	3	4	5	6	7	8	9	$10 \le m \le 17$
$L(m,17)$	1	1	1	1	3	6	2	2	0	0
$+2m \cdot 2^{L(m,17)}$	4	8	12	16	80	—	—	—	—	—
$-2m \cdot 2^{L(m,17)}$	—	—	—	—	—	-768	-56	-64	-18	$-2m$
$p(\overline{J_2}^{-1},17)(m)$	4	8	12	16	10	2	14	6	17	$29-2m$

Then $p(\overline{J_2}^{-1},17) =$ (1 17 9 13 11 12 3 16 4)(2 6 8)(5 15 10)(7 14) and 17 does not belong to $P(\overline{J_2}^{-1})$. □

As in the previous section it is possible to "invert" the two algorithms for $p(\overline{J_2}^{-1},n)$. This yields

$N := 2*n+1-m$;
while N is odd **do** $N := (2*n+1-N)/2$;
$p(\overline{J_2},n)(m) := N/2$

and, respectively,

$D := m$;
while D is even **do** $D := (-D/2) \bmod (2*n+1)$;
$p(\overline{J_2},n)(m) := (2*n+1-D)/2$.

Example 6.8. Executing these algorithms with $n = 14$ and $m = 7$, results in $N = 22$ and $D = 7$; then the loops will be skipped and $p(\overline{J_2},14)(7) = 11$. Starting the first algorithm with $m = 14$, produces successive N-values: 15, 7, 11, 9 and 10 such that $p(\overline{J_2},14)(14) = 5$. The second algorithm gives for $m = 14$ as D-values: 14, 22, 18, 20 and 19 and we also obtain $p(\overline{J_2},14)(14) = 5$; cf. Example 6.4. □

From the latter algorithm we obtain the following closed form for the permutation $p(\overline{J_2}, n)$:

$$p(\overline{J_2}, n)(m) = (2n + 1 - \llbracket m \rrbracket^-_{2n+1})/2 \qquad (1 \leq m \leq n),$$

where $\llbracket x \rrbracket^-_u$ is the odd number such that $1 \leq \llbracket x \rrbracket^-_u < u$ and $x \equiv \llbracket x \rrbracket^-_u (-2)^t \pmod{u}$ for the smallest $t \geq 0$. As examples, we mention that $\llbracket 6 \rrbracket^-_{29} = 21$ and $\llbracket 2 \rrbracket^-_{35} = 23$, since $6 \equiv 21(-2)^3 \pmod{29}$ with $t = 3$, and $2 \equiv 23(-2)^6 \pmod{35}$ with $t = 6$, respectively. Clearly, for each odd x with $1 \leq x < u$, we have $\llbracket x \rrbracket^-_u = x$ as $t = 0$ applies.

Returning to Example 6.7, we observe that these t-values coincide with the values of $L(m, n)$, i.e., the number of times the loop in the algorithm has to be executed. Therefore we leave it as an exercise to the reader to compute $p(\overline{J_2}, 14)$ and $p(\overline{J_2}, 17)$: Examples 6.7 and 6.8 may be used to check the results of these computations.

In applications the closed form for $p(\overline{J_2}^{-1}, n)$ is much more convenient than the one for $p(\overline{J_2}, n)$; we encountered a similar situation in the previous section. Therefore we will proceed as in Section 5; we formulate our results in terms of $\overline{J_2}$, but in our proofs we apply $\overline{J_2}^{-1}$ or $p(\overline{J_2}^{-1}, n)$. And, of course, we rely on the equality $P(\overline{J_2}) = P(\overline{J_2}^{-1})$: a number is a $\overline{J_2}$-prime if and only if it is a $\overline{J_2}^{-1}$-prime.

For the set of $\overline{J_2}$-primes or, equivalently, the set of $\overline{J_2}^{-1}$-primes we have

$$P(\overline{J_2}) = \{2,\ 3,\ 6,\ 11,\ 14,\ 18,\ 23,\ 26,\ 30,\ 35,\ 39,\ 50,\ 51,\ 74,\ 83,\ 86,\ 90,\ 95,\ 98,\ 99,\ 119,\\ 131,\ 134,\ 135,\ 146,\ 155,\ 158,\ 174,\ 179,\ 183,\ 186,\ 191,\ 194,\ 210,\ 230,\ 231, \ldots\}.$$

In [25] this integer sequence is known as A163781*.

The first step in the characterization of $\overline{J_2}$-primes is a counterpart of Lemma 5.6; viz.

Lemma 6.9. *For each integer n in $\mathbb{N}_2$ with $n \not\equiv 1 \pmod 3$,*

$$\sum_{i=1}^{\lfloor n/3 \rfloor} \left\lfloor \lg \frac{4n+2}{2n+1-6i} \right\rfloor_O + \sum_{i=\lfloor n/3 \rfloor + 1}^{n} \left\lceil \lg \frac{n+2}{6i-2n-1} \right\rceil_E = n.$$

Proof. Our argument used in the alternative proof of Lemma 5.6 can be applied here as well: the sum equals $\sum_{m=1}^{n} L(m, n) = C(2n, n) = n$. (A lengthy proof in the style of [12], such as our first proof of Lemma 5.6, is left as an exercise to the reader.)

Note that the condition $n \not\equiv 1 \pmod 3$ is crucial: if $n \equiv 1 \pmod 3$, then this sum equals $C(2n-1, n) = n - 1$, since we construct in that case n chains using $2n-1$ points only in the numbering process; cf. Example 6.5. □

The next three results can be proved in way very similar to Proposition 5.8, Lemma 5.9 and Proposition 5.10, respectively. Of course, we use Lemma 6.9 instead of Lemma 5.6 in establishing Proposition 6.10.

Proposition 6.10. *If n in $\mathbb{N}_2$ is $\overline{J_2}$-prime, then for each m $(1 \leq m < 2n+1)$:*

(1) *If $n \equiv 2 \pmod 4$, then $m \cdot 2^n \equiv -m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv -m \pmod{2n+1}$.*

(2) *If $n \equiv 3 \pmod 4$, then $m \cdot 2^n \equiv +m \pmod{2n+1}$ and $m \cdot (-2)^n \equiv -m \pmod{2n+1}$.* □

Lemma 6.11. *If there exist integers x and y with $x, y \geq 1$ such that $n = 2xy + x + y$, then n is not $\overline{J_2}$-prime.*

Proof. We adapt the proof of Lemma 5.9; see also the proof of Lemma 3.7. First, notice that for $n \not\equiv 1 \pmod 3$, the permutation $p(\overline{J_2}^{-1}, n)$ may be written as

$$p(\overline{J_2}^{-1}, n)(m) = (2n+1) \cdot c_{m,n} + 2m \cdot 2^{\left\lfloor \lg \frac{4n+2}{2n+1-6m} \right\rfloor_O} \qquad \text{if } 1 \leq m \leq u = \lfloor n/3 \rfloor,$$

$$p(\overline{J_2}^{-1}, n)(m) = (2n+1) \cdot c_{m,n} - 2m \cdot 2^{\left\lceil \lg \frac{n+2}{6m-2n-1} \right\rceil_E} \qquad \text{if } u < m \leq n,$$

where the $c_{m,n}$ $(1 \leq m \leq n)$ are appropriately chosen constants. Secondly, we observe that if $n = 2xy + x + y$, then $2n + 1 = 4xy + 2x + 2y + 1 = (2x + 1)(2y + 1)$.

Now it is straightforward to show that $p(\overline{J_2}^{-1}, n)$ maps multiples of $2x{+}1$ on multiples of $2x{+}1$. Then the statement follows as in the proofs of Lemma 3.7 and 5.9. □

Proposition 6.12. *If n is $\overline{J_2}$-prime, then $2n + 1$ is a prime number.* □

The cases in Proposition 6.10, that have been omitted, are dealt with in Theorem 6.13; cf. Theorem 5.11.

Theorem 6.13. *Let n be a number in $\mathbb{N}_2$. If $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$, then n is not $\overline{J_2}$-prime.*

Proof. Assuming —similar to the proof of Theorem 5.11— that $n = 4k$ or $n = 4k + 1$ $(k \geq 1)$ is $\overline{J_2}$-prime implies that, by Proposition 6.12, $p = 2n{+}1$ is a prime number and that -2 is quadratic residue of p (Proposition 3.12). Then again it is straightforward to derive contradictions as in the proofs of Theorems 3.13 and 5.11. □

Next we arrive at the main result of this section.

Theorem 6.14. *A number n is $\overline{J_2}$-prime if and only if $2n + 1$ is a prime number and exactly one of the following two conditions holds:*

(1) *$n \equiv 2 \pmod 4$ and both -2 and $+2$ generate the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

(2) *$n \equiv 3 \pmod 4$ and -2 generates the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$ but $+2$ does not.*

Proof. The argument is almost identical to the proofs of Theorems 3.15 and 5.12. But now we use Propositions 6.10 and 6.12 (instead of Propositions 3.4 and 3.8, respectively 5.8 and 5.10) and Theorem 6.13 (instead of Theorems 3.13, respectively 5.11). □

Example 6.15 (1) Of course, 17 is not $\overline{J_2}$-prime because 35 is not a prime number; cf. Example 6.7.

(2) When $n = 14$, condition (1) of Theorem 6.14 applies; cf. Examples 6.3 and 6.7.

(3) For $n = 11$, we have $11 \equiv 3 \pmod 4$, 23 is a prime number, and -2 belongs to the set $\{-9, -8, -6, -4, -3, -2, 5, 7, 10, 11\}$ of possible generators of $\mathbb{Z}^\star_{23}$; so 11 is $\overline{J_2}$-prime. □

As to be expected, we now can combine Theorem 6.14 with the characterization results of Section 4.

N	$\pi(S,N)$	$\pi(\overline{S},N)$	$\pi(T,N)$	$\frac{\pi(S,N)}{\pi(T,N)}$	$\frac{\pi(\overline{S},N)}{\pi(T,N)}$
10^1	3	2	5	0.60000	0.40000
10^2	13	12	30	0.43333	0.40000
10^3	67	69	177	0.37853	0.38983
10^4	470	465	1257	0.37391	0.36993
10^5	3603	3612	10084	0.35730	0.35819
10^6	29341	29438	83584	0.35104	0.35220
10^7	248491	248761	713154	0.34844	0.34882
10^8	2154733	2153846	6214402	0.34673	0.34659

Table 2: Counting X-primes with $X \in \{S, \overline{S}, T\}$.

Theorem 6.16. *A number n is $\overline{J_2}$-prime if and only if either n is A_0-prime or n is A_1^--prime: $P(\overline{J_2}) = P(A_0) \cup P(A_1^-)$. Equivalently, a number n is $\overline{J_2}$-prime if and only if $2n+1$ is a prime number and -2 generates the multiplicative group $\mathbb{Z}^\star_{2n+1}$ of $\mathbb{Z}_{2n+1}$.*

Proof. Theorems 4.4, 4.9 and 6.14. □

Corollary 6.17. $P(\overline{J_2}) = H(\overline{S})$.

Proof. Theorems 4.10(2) and 6.16. □

In conclusion, we remark that the permuting operation $\overline{J_2}$ is indeed a dual of the permuting operation J_2, since we have —with Definition 6.1 in mind— that $K = 2$, $\gamma(n) = 2n+1$, $M(1) = 1$, $M(2) = 2$, $N(1) = 1$, $N(2) = 0$, $g_{1,1} = +2$, $h_{1,1} = -2$, $g_{2,1} = +2$, $g_{2,2} = -2$, and $\varphi(P_i) = Q_i$ $(i = 1, 2)$ with

J_2	$\overline{J_2}$
$P_1(n)$ is "$n \equiv 1 \pmod{2n+1}$"	$Q_1(n)$ is "$n \equiv 3 \pmod{2n+1}$"
$P_2(n)$ is "$n \equiv 2 \pmod{2n+1}$"	$Q_2(n)$ is "$n \equiv 2 \pmod{2n+1}$".

7 Concluding Remarks

7.1 General

In the previous sections we studied some permuting operations on strings and focussed our attention to the corresponding permutations and their primes. The Josephus operations J_k $(k \geq 3)$ seem to be intractable in the sense that is hard to establish any of their

N	$\pi(A_0,N)$	$\pi(A_1,N)$	$\pi(A_1^+,N)$	$\pi(A_1^-,N)$	$\frac{\pi(A_0,N)}{\pi(T,N)}$	$\frac{\pi(A_1^+,N)}{\pi(T,N)}$	$\frac{\pi(A_1^-,N)}{\pi(T,N)}$
10^1	2	3	2	1	0.40000	0.40000	0.20000
10^2	11	19	10	9	0.36667	0.33333	0.33333
10^3	61	116	55	61	0.34463	0.31073	0.34463
10^4	418	839	421	418	0.33254	0.33492	0.33254
10^5	3378	6706	3328	3378	0.33499	0.33003	0.33499
10^6	27882	55702	27861	27841	0.33358	0.33333	0.33309
10^7	237676	475478	237656	237822	0.33327	0.33325	0.33348
10^8	2071170	4143232	2072304	2070928	0.33329	0.33347	0.33325

Table 3: Counting X-primes with $X \in \{A_0, A_1, A_1^+, A_1^-\}$.

structural properties, a phenomenon already suggested in Section 1.3 of [12][6]. In addition, for $k \geq 3$, the J_k-primes are rather scarce, and the computation of the sets $P(J_k)$ is quite time consuming.

So the most intriguing permuting operations that we discussed, are S, $\overline{S}$, T, A_0, A_1, A_1^+, A_1^-, J_2 and $\overline{J_2}$. Although defined quite differently, they are interconnected by Theorems 4.3, 4.10, 5.13 and 6.15 as well as Corollaries 5.14 and 6.16. Summarizing, we have:

$$P(J_2) = H(S) = P(A_0) \cup P(A_1^+),$$
$$P(\overline{J_2}) = H(\overline{S}) = P(A_0) \cup P(A_1^-),$$

and

$$P(T) = P(A_0) \cup P(A_1^+) \cup P(A_1^-)$$

in which $P(A_0)$, $P(A_1^+)$ and $P(A_1^-)$ are mutually disjoint sets. This implies that

$$P(T) = P(J_2) \cup P(\overline{J_2}) = H(S) \cup H(\overline{S})$$

with

$$P(J_2) \cap P(\overline{J_2}) = H(S) \cap H(\overline{S}) = P(A_0).$$

For the corresponding sets of primes we obtained characterization results in Sections 2–6. It is evident that the set of T-primes (or Queneau numbers) and some of its subsets deserve much more attention than they received up to now [7, 8].

It is also clear that X-primes (for X is equal to S, $\overline{S}$, T, A_0, A_1, A_1^+, A_1^-, J_2 or $\overline{J_2}$) are related in some specific way to (ordinary) prime numbers; cf. Theorems 2.10, 3.15, 4.4, 4.5,

[6]The only two obvious exceptions are: (i) for even k, $P(J_k)$ contains the number 2, and (ii) for odd k, $P(J_k)$ contains odd numbers only. Now (i) is almost trivial and (ii) is rather straightforward to prove; see also Exercise 7 in [15].

N	$\pi(J_2,N)$	$\pi(\overline{J_2},N)$	$\pi(\overline{S}',N)$	$\pi(S',N)$	$\frac{\pi(J_2,N)}{\pi(T,N)}$	$\frac{\pi(\overline{J_2},N)}{\pi(T,N)}$
10^1	4	3	4	3	0.80000	0.60000
10^2	21	20	16	5	0.70000	0.66667
10^3	116	122	75	7	0.65537	0.68927
10^4	839	836	473	9	0.66746	0.66508
10^5	6706	6756	3622	11	0.66501	0.66997
10^6	55743	55723	29450	13	0.66691	0.66667
10^7	475332	475498	248775	15	0.66652	0.66675
10^8	4143474	4142098	2153862	17	0.66675	0.66653

Table 4: Counting X-primes with $X \in \{J_2, \overline{J_2}, \overline{S}', S'\}$.

4.8, 4.9, 5.12 and 6.14. So let us count the several X-primes in a way similar to counting (ordinary) prime numbers (as in e.g. [26] §1.5) and have a look at their distributions.

7.2 Distribution of X-primes

Let $\pi(X,N)$ be the number of X-primes in the interval $2 \leq n \leq N$. We write $\pi(N)$ instead of $\pi(X,N)$ whenever the permuting operation X is clear from the context. Then our counting results can be summarized as in Tables 2–4.

In Tables 2 and 3 we see that $\pi(A_0,N) + \pi(A_1,N) = \pi(T,N)$, which is in accordance with Theorem 4.3. And there are approximately twice as many A_1-primes as A_0-primes in each interval. Similarly, in Table 3 we observe that $\pi(A_1^+,N) + \pi(A_1^-,N) = \pi(A_1,N)$ (cf. Definition 4.7), and that there are approximately as many A_1^+-primes as A_1^--primes in each interval. Though there are no T-primes n with $n \equiv 0 \pmod 4$, the remaining three cases seem to be equally distributed: there are approximately as many A_1^+-primes (T-primes n with $n \equiv 1 \pmod 4$) as A_0-primes (T-primes n with $n \equiv 2 \pmod 4$) as A_1^--primes (T-primes n with $n \equiv 3 \pmod 4$). Then it is no surprise that there approximately as many J_2-primes as $\overline{J_2}$-primes in each interval, as $P(J_2) = P(A_0) \cup P(A_1^+)$ and $P(\overline{J_2}) = P(A_0) \cup P(A_1^-)$; cf. Tables 3 and 4.

Tables 5, 6 and 7 show that the distributions of the S-, $\overline{S}$, T-, A_0-, A_1-, A_1^+-, A_1^--, J_2- and $\overline{J_2}$-prime numbers exhibits a "Prime Number Theorem-like" behavior. Remember that the Prime Number Theorem reads as:

Prime Number Theorem. *The number $\pi(N)$ of prime numbers less than or equal to N is asymptotic to $N/\ln N$. That is* $\lim_{N\to\infty} \pi(N) \ln N/N = 1$. □

But the distributions of X-primes show limiting values $\Lambda_X = \lim_{N\to\infty} \pi(X,N) \ln N/N$ unequal to 1; rough estimates of Λ_X are in Table 9.

	Shuffle S		Shuffle $\overline{S}$		Twist T	
N	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$
10^1	3	0.69077553	2	0.46051702	5	1.15129255
10^2	13	0.59867212	12	0.55262042	30	1.38155106
10^3	67	0.46281960	69	0.47663511	177	1.22267268
10^4	470	0.43288600	465	0.42828083	1257	1.15773978
10^5	3603	0.41481070	3612	0.41584687	10084	1.16096340
10^6	29341	0.40536090	29438	0.40670100	83584	1.15475563
10^7	248491	0.40052017	248761	0.40095536	713154	1.14946844
10^8	2154733	0.39691649	2153846	0.39675310	6214402	1.14473515

Table 5: Distribution of S-, $\overline{S}$- and T-primes.

This comparison also suggests another question: does there exist a permuting operation X_p on strings such that $P(X_p)$ equals the set of prime numbers? Phrased in this way, the question is easy to answer: define X_p by

$X_p(w) = \sigma(w)$ if the length of w is a prime number,

$X_p(w) = \lambda(w) = w$ otherwise;

cf. Example 1.1 for the definitions of σ and λ. Thus we should exclude any form of (hidden) primality testing in the definition of X_p in order to keep this question nontrivial.

7.3 Twin X-primes

Looking somewhat closer to the set of S-primes, we see a number of pairs of twin S-primes, i.e., of pairs $(n, n{+}2)$ with both n and $n{+}2$ being S-prime: (2, 4), (10, 12), (58, 60), (178, 180), (346, 348), (418, 420), (658, 660), (826, 828), (1450, 1452), (1618, 1620), etc.

In case of $\overline{S}$ we have a similar situation; the first few twin $\overline{S}$-primes (i.e., pairs $(n, n{+}2)$ with both n and $n{+}2$ being $\overline{S}$-prime) are: (4, 6), (100, 102), (196, 198), (268, 270), (460, 462), (820, 822), (1060, 1062), (1228, 1230), (1276, 1278) and (1300, 1302).

For T-primes there is even an abundance of twin T-primes, i.e., of pairs $(n, n{+}1)$ with both n and $n{+}1$ being T-prime: (2, 3), (5 , 6), (29, 30), (50, 51), (89, 90), (98, 99), (134, 135), (173, 174), (209, 210), (230, 231), (329, 330), (410, 411), (413, 414), (530, 531), (614, 615), (638, 639), (650, 651), (725, 726), etc.

But for $X \in \{A_0, A_1, A_1^+, A_1^-\}$ there are no twin X-primes (i.e., pairs $(n, n{+}1)$ with both n and $n{+}1$ being X-prime): in these cases the gap between two consecutive X-primes is at least 4 (for A_0, A_1^+ and A_1^-) or 2 (for A_1). On the other hand there exist twin J_2-

	Archimedes A_1		Archimedes A_1^+		Archimedes A_1^-	
N	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$
10^1	3	0.69077553	2	0.46051702	1	0.23025851
10^2	19	0.87498234	10	0.46051702	9	0.41446532
10^3	116	0.80129961	55	0.37992654	61	0.42137307
10^4	839	0.77274756	421	0.38775533	418	0.38499223
10^5	6706	0.77205678	3328	0.38315016	3378	0.38890662
10^6	55702	0.76955157	27861	0.38491394	27841	0.38463763
10^7	475478	0.76637999	237656	0.38305621	237822	0.38332377
10^8	4143232	0.76321154	2072304	0.38173250	2070928	0.38147904

Table 6: Distribution of A_1-, A_1^+- and A_1^--primes.

primes (i.e., pairs $(n,\ n{+}1)$ with both n and $n{+}1$ being J_2-prime): (5 , 6), (29, 30), (89, 90), (173, 174), (209, 210), (329, 330), etc. And there are twin $\overline{J_2}$-primes (i.e., pairs $(n,\ n{+}1)$ with both n and $n{+}1$ being $\overline{J_2}$-prime): (2, 3), (50, 51), (98, 99), (134, 135), (230, 231), (410, 411), etc.

Obviously, this leads to

Conjecture 7.1.

(1) **Weak Twin S-prime Conjecture.** *There exists an infinite number of twin S-primes (pairs of numbers $(n,\ n{+}2)$ with both n and $n{+}2$ being S-prime).*

(2) **Weak Twin $\overline{S}$-prime Conjecture.** *There exists an infinite number of twin $\overline{S}$-primes (pairs of numbers $(n,\ n{+}2)$ with both n and $n{+}2$ being $\overline{S}$-prime).*

(3) **Weak Twin T-prime Conjecture.** *There exists an infinite number of twin T-primes (pairs of numbers $(n,\ n{+}1)$ with both n and $n{+}1$ being T-prime).*

(4) **Weak Twin J_2-prime Conjecture.** *There exists an infinite number of twin J_2-primes (pairs of numbers $(n,\ n{+}1)$ with both n and $n{+}1$ being J_2-prime).*

(5) **Weak Twin $\overline{J_2}$-prime Conjecture.** *There exists an infinite number of twin $\overline{J_2}$-primes (pairs of numbers $(n,\ n{+}1)$ with both n and $n{+}1$ being $\overline{J_2}$-prime).* □

Notice that if $(2n,\ 2n{+}2)$ is a pair of twin S-primes or a pair of twin $\overline{S}$-primes, then by Proposition 3.3 $(n,\ n{+}1)$ is a pair of twin T-primes. Conversely, by Theorems 4.3, 4.4, 4.5 and 4.10 we have that if $(n,\ n{+}1)$ is a pair of twin T-primes, then $(2n,\ 2n{+}2)$ is either a pair of twin S-primes or a pair of twin $\overline{S}$-primes.

From Proposition 3.3, Theorems 4.10, 5.14 and 6.15 it follows that any of Conjectures 7.1(1), 7.1(2), 7.1(4) or 7.1(5) implies Conjecture 7.1(3).

	Archimedes A_0		Josephus J_2		Josephus $\overline{J_2}$	
N	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$
10^1	2	0.46051702	4	0.92103404	3	0.69077553
10^2	11	0.50656872	21	0.96708574	20	0.92103404
10^3	61	0.42137307	116	0.80129961	122	0.84274614
10^4	418	0.38499223	839	0.77274756	836	0.76998446
10^5	3378	0.38890662	6706	0.77205678	6756	0.77781324
10^6	27882	0.38520407	55743	0.77011800	55723	0.76984169
10^7	237676	0.38308845	475332	0.76614466	475498	0.76641222
10^8	2071170	0.38152361	4143474	0.76325612	4142098	0.76300265

Table 7: Distribution of A_0-, J_2 and $\overline{J_2}$-primes.

Very likely, any of Conjectures 7.1(1)-(5) is extremely hard to prove, since with Propositions 2.5, 3.8, 5.10 and 6.12 respectively, they imply the well-known, long open standing

Weak Twin Prime Conjecture. *There exists an infinite number of twin primes (pairs of numbers* $(p,\ p{+}2)$ *with both* p *and* $p{+}2$ *being prime numbers).* □

There exist pairs of twin primes $(p,\ p{+}2)$ for which there is no "corresponding" pair of twin S-primes, or of twin $\overline{S}$-primes (viz. $(n,\ n{+}2)$ with $n = p-1$) and no pair of T-primes, or of J_2-primes or of $\overline{J_2}$-primes (viz. $(n,\ n{+}1)$ with $n = (p-1)/2$); the first few examples are (5, 7), (17, 19), (29, 31) and (41, 43).

7.4 Related permutations and their primes

As to be expected changing the definitions, even slightly, gives rise to other sets of primes with different properties and their own, typical distributions. We only present two obvious examples: $\overline{S}'$ and S'. Their distributions are in Table 8.

Slightly varying $p(\overline{S}, n)$ yields $p(\overline{S}', n)$, defined by

$$p(\overline{S}', n)(m) = n + 1 - 2m \qquad \text{if } 1 \le m < k = \lceil (n+1)/2 \rceil, \text{ and}$$
$$p(\overline{S}', n)(m) = n - 2(m-k) \qquad \text{if } k \le m \le n.$$

Note that for even n, $p(\overline{S}', n)(m) = p(\overline{S}, n)(m) \equiv -2m \pmod{n{+}1}$, and for odd n, $p(\overline{S}', n)(n) = 1 \ne n = p(\overline{S}, n)(n)$. Now we have

$$P(\overline{S}') = \{3,\ 4,\ 6,\ 9,\ 12,\ 22,\ 27,\ 28,\ 36,\ 46,\ 52,\ 60,\ 70,\ 78,\ 81,\ 100,\ 102,\ 148,\ 166,\ 172,$$
$$180,\ 190,\ 196,\ 198,\ 238,\ 243,\ 262,\ 268,\ 270,\ 292,\ 310,\ 316,\ 348,\ 358,\ \ldots\}.$$

	Shuffle $\overline{S}'$		Shuffle S'	
N	$\pi(N)$	$\pi(N)\ln N/N$	$\pi(N)$	$\pi(N)\ln N/N$
10^1	4	0.92103404	3	0.69077553
10^2	16	0.73682723	5	0.23025851
10^3	75	0.51808165	7	0.04835429
10^4	473	0.43564910	9	0.00828931
10^5	3622	0.41699816	11	0.00126642
10^6	29450	0.40686679	13	0.00017960
10^7	248775	0.40097792	15	0.00002418
10^8	2153862	0.39675604	17	0.00000313

Table 8: Distribution of $\overline{S}'$- and S'-primes.

A further modification of $p(\overline{S}', n)$ results in $p(S', n)$, defined by,

$$p(S', n)(m) = n + 2 - 2m \qquad \text{if } 1 \leq m \leq k = \lceil n/2 \rceil, \text{ and}$$
$$p(S', n)(m) = n + 1 - 2(m - k) \qquad \text{if } k < m \leq n.$$

The corresponding set of S'-primes exhibits a remarkable regularity; cf. Conjecture 7.2(3) below:

$$P(S') = \{2, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, 177147, 531441, \ldots\}.$$

7.5 Miscellaneous

Readers interested in extending the results of the present paper may start to prove (in a way similar as we did in Sections 2–4) some observations collected in:

Conjecture 7.2.
(1) *A number n in $\mathbb{N}_2$ is $\overline{T}$-prime if and only if n is T-prime.*

(2) *A number n in $\mathbb{N}_2$ is $\overline{S}'$-prime if and only if either n is an $\overline{S}$-prime or n is equal to 3^k for some $k \geq 1$. Equivalently, $P(\overline{S}') = P(\overline{S}) \cup \{3^k | k \geq 1\}$.*

(3) *A number n in $\mathbb{N}_2$ is S'-prime if and only if either n equals 2 or n is equal to 3^k for some $k \geq 1$. Equivalently, $P(S') = \{2\} \cup \{3^k | k \geq 1\}$.* □

For the definitions of $\overline{T}$, $\overline{S}'$ and S', we refer to Sections 3 and 7.4.

In this context we also recall the problem mentioned in Section 7.2: the characterization of the ordinary prime numbers as primes of a certain permuting operation.

X	S	$\overline{S}$	T	A_0	A_1	A_1^+	A_1^-	J_2	$\overline{J_2}$	$\overline{S}'$	S'
Λ_X	0.37	0.37	1.12	0.37	0.74	0.37	0.37	0.74	0.74	0.37	0.00

Table 9: Limit values Λ_X (rough estemates).

Those readers who are interested in this type of problems, are also referred to [6] which contains for each permuting operation X from $\{S, T, A_0, A_1, A_1^+, A_1^-, J_2, \overline{S}, \overline{S}', S'\}$,

- the elements of $P(X)$ in the interval $2 \leq n \leq 10000$,
- the cycle structure representation of all permutations $p(X, n)$ with $2 \leq n \leq 1000$,

and some additional material.

Finally we remark that, apart from determining the sets $P(J_k)$ for $k \geq 3$ (table 1), the computation of the entries in Tables 2–8 (and similar tables) is a very time consuming task as well, especially when N becomes larger and larger. We did not rely on sieves or any other advanced techniques; we only applied a bit of filtering. Viz. for $P(S)$ and $P(A_0)$ we restrict our attention to the even numbers, for $P(A_1)$ to the odd numbers, for $P(A_1^+)$ and $P(A_1^-)$ to numbers congruent 1 and 3 modulo 4 respectively, and for $P(T)$ to the numbers $n \equiv 2, 3, 5, 6, 9, 11 \pmod{12}$.

Acknowledgement. I am much indebted to Hendrik W. Lenstra Jr. who made some useful comments on a very preliminary version of this paper.

References

1. J.A. Anderson & J.M. Bell, *Number Theory with Applications* (1997), Prentice-Hall, Upper Saddle River, NJ.
2. P.R.J. Asveld, Generating all permutations by context-free grammars in Chomsky normal form, *Theoret. Comput. Sci.* **354** (2006) 118–130.
3. P.R.J. Asveld, Generating all cyclic shifts by context-free grammars in Chomsky normal form, *J. Autom. Lang. Comb.* **11** (2006) 147–159.
4. P.R.J. Asveld, Generating all circular shifts by context-free grammars in Greibach normal form, *Internat. J. Found. of Comput. Sci.* **18** (2007) 1139–1149.
5. P.R.J. Asveld, Generating all permutations by context-free grammars in Greibach normal form, *Theoret. Comput. Sci.* **409** (2008) 565–577.
6. P.R.J. Asveld, Some families of permutations and their primes, TR-CTIT-09-27, Dept. of Computer Science, Twente University of Technology, Enschede, The Netherlands, `http://eprints.eemcs.utwente.nl/15678/`

7. M. Bringer, Sur un problème de R. Queneau, *Math. Sci. Humaines* **27** (1969) 13–20.
8. C.W. Carroll & W.F. Orr, On the generalization of the sestina, *Delta (Waukesha)* **5** (1975) 32–44.
9. J. Dowdy & M.E. Mays, Josephus permutations, *J. Combin. Math. Combin. Comput.* **6** (1989) 125–130.
10. J.-G. Dumas, Caractérisation des quenines et leur représentation spirale, *Math. Sci. Humaines/Math. Soc. Sci.* **184** (2008) 9–23.
11. J.-G. Dumas, personal communication (September 4, 2009).
12. R.L. Graham, D.E. Knuth & O. Patashnik, *Concrete Mathematics* (1989), Addison-Wesley, Reading, MA.
13. L. Halbeisen & N. Hungerbühler, The Josephus problem, *J. Théor. Nombres Bordeaux* **9** (1997) 303–318.
14. G.H. Hardy & E.M. Wright, *An Introduction to the Theory of Numbers* (1938), Fourth edition (1959), Oxford University Press, Oxford, UK.
15. I.N. Herstein & I. Kaplansky, *Matters Mathematical* (1974), Harper & Row, New York.
16. M. Jantzen, The power of synchronizing operations on strings, *Theoret. Comput. Sci.* **14** (1981) 127–154.
17. M. Jantzen, Hierarchies of principal twist-closed trios, *STACS* 98, Lect. Notes in Comput. Sci. **1373** (1998) Springer, Berlin, pp. 344–355.
18. M. Jantzen & A. Kurgansky, Refining the hierarchy of blind multicounter languages and twist-closed trios, *Inform. Comput.* **185** (2003) 158–181.
19. M. Lothaire, *Combinatorics on Words* (1983), Addison-Wesley, Reading, MA.
20. R.A. Mollin, *Fundamental Number Theory with Applications* (1998), CRC Press, Boca Raton, FL.
21. A.M. Odlyzko & H.S. Wilf, Functional iteration and the Josephus problem, *Glasgow Math. J.* **33** (1991) 47–61.
22. R. Queneau, *Bâtons, chiffres et lettres* (1965), Gallimard, Paris.
23. R. Queneau, Note complémentaire sur la sextine, *Subsidia Pathaphysica* Troisième et nouvelle série (1965) No. 1, 79–80.
24. P. Schumer, The Josephus problem; once more around, *Math. Mag.* **75** (2002) 12–17.
25. N.J.A. Sloane, *On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/Seis.html`
An earlier, non-electronic version appeared as: N.J.A. Sloane & S. Plouffe, *The Encyclopedia of Integer Sequences* (1995), Academic Press, San Diego CA, etc.
26. S.Y. Yan, *Number Theory for Computing* (2000), Springer-Verlag, Berlin – Heidelberg – New York.