Permuting Operations on Strings and Their Relation to Prime Numbers

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 — Some length-preserving operations on strings only permute the symbol positions in strings; such an operation X gives rise to a family $\{X_n\}_{n\geq 2}$ of similar permutations. We investigate the structure and the order of the cyclic group generated by X_n. We call an integer n *X-prime* if 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. Here X and X' range over well-known examples (reversal, cyclic shift, shuffle, twist) and some new ones based on Archimedes spiral and on the Josephus problem.

Keywords: operation on strings, shuffle, twist, prime number, Josephus problem, Queneau number.

1 Introduction

In discrete mathematics and in theoretical computer science many operations on strings have been studied [11, 17]. This paper is devoted to the subclass of length-preserving operations that only permute the symbol positions in the string. In this section we discuss some simple examples and we illustrate the properties of the permutations that are associated to these operations. Then in the next sections we turn our attention to more interesting, length-preserving permuting operations. 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 [17].

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 (families of) 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: $\lambda(\alpha_n) = a_1 a_2 \cdots a_n$.
(b) Consider the transposition of the first two symbols: $\tau(\alpha_n) = a_2 a_1 a_3 \cdots a_n$.
(c) ρ denotes the *reversal* or *mirror* operation: $\rho(\alpha_n) = a_n a_{n-1} \cdots a_2 a_1$.
(d) σ is the *cyclic* or *circular shift*: $\sigma(\alpha_n) = a_2 a_3 \cdots a_n a_1$.
Clearly, λ, τ, ρ and σ are permuting operations. □

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

Henceforth, we describe permutations by their complete cycle structure representation.

Example 1.1. (continued). (a) $\lambda_n = (1)(2)(3)\cdots(n)$.
(b) $\tau_n = (1\,2)(3)(4)\cdots(n)$.
(c) $\rho_n = (1\ \ n)(2\ \ n{-}1)(3\ \ n{-}2)\cdots(n/2\ \ n/2{+}1)$ if n is even, and
$\rho_n = (1\ n)(2\ \ n{-}1)(3\ \ n{-}2)\cdots((n{-}1)/2\ \ \ (n{+}3)/2)((n{+}1)/2)$ if n is odd.
(d) $\sigma_n = (1\ \ n\ \ n{-}1\ \ n{-}2\ \ \cdots\ \ 3\ \ 2)$. □

Definition 1.2. Let X be a permuting operation. A number n ($n \in \mathbb{N}_2$) is called *X-prime* if 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. □

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 characterize the sets $P(X)$ and we investigate the structure of the elements in $\{X_n\}_{n\geq 2}$. 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.

2 The Shuffle Operation and Its Primes

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 $S_\bullet$ to the standard word α_n results in $S_\bullet(\alpha_n) = a_1 a_k a_2 a_{k+1} a_3 a_{k+2} \cdots$ where $k = \lceil (n+1)/2 \rceil$.

Interleaving and shuffling play an important part in describing synchronization aspects of parallel processes; cf. e.g. [14].

$S_\bullet$ leaves the position of a_1 in α_n unchanged and so $P(S_\bullet) = \varnothing$. The situation becomes less trivial when we modify $S_\bullet$ slightly: before the interleaving of the two halves of the card deck we interchange the two parts. The resulting 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 [13]. For the permutations S_n induced by the shuffle operation S we have

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

Thus, if $S_n = c_1c_2\cdots c_k$ (each c_i is a cycle), then $S_{n+1} = c_1c_2\cdots c_k(n{+}1)$. Consequently, all S-primes are even:

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

This happens to be the integer sequence A071642 in [22].

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 $n = 8$ and $n = 10$, we obtain respectively: $S_8 = (1\,2\,4\,8\,7\,5)(3\,6)$, $\#\langle S_8\rangle = 6$, $8 \notin P(S)$, $S(\alpha_{10}) = a_6a_1a_7a_2a_8a_3a_9a_4a_{10}a_5$, $S_{10} = (1\,2\,4\,8\,5\,10\,9\,7\,3\,6)$, $\#\langle S_{10}\rangle = 10$, and hence $10 \in P(S)$. □

As $S_n^n(m) = m$, we have for even n, $m \cdot 2^n \equiv m \pmod{n+1}$ $(1 \le m \le n)$. Remember that ρ is the reversal 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 $\#\langle S_n\rangle < n$ which contradicts the fact that n is S-prime.

Then, according to pp. 128–129 in [11], 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 $\#\langle S_n\rangle = n/2$ 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 $S_n^{n/2}(m) \equiv -m \pmod{n+1}$ or, equivalently, $S_n^{n/2}(m) = n+1-m$ 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 and 2.2.3 in [18] or Theorem 3.52 in [1].

Theorem 2.4. *The number p is a 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 $S_n^0(1)$, $S_n^1(1)$, $S_n^2(1)$, …, $S_n^{n-1}(1)$— are equal to 1, 2, 3, …, n in some order. When we multiply them, we obtain

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

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. □

In order to characterize $P(S)$ we need the following notation. As usual $\mathbb{Z}$ denotes the set of all integers. For a prime number p, $\mathbb{Z}_p$ denotes the finite (or Galois) field of integers

modulo p —i.e., $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$— and $\mathbb{Z}_p^\star$ the cyclic multiplicative group of $\mathbb{Z}_p$. By G_p we denote the set of possible generators of $\mathbb{Z}_p^\star$.

Theorem 2.6. *A number n is S-prime if and only if $n{+}1$ is an odd prime number and $+2$ generates $\mathbb{Z}_{n+1}^\star$.*

Proof. If n is S-prime, then n is even and $n{+}1$ is an odd prime (Proposition 2.5). 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., $+2$ generates $\mathbb{Z}_p^\star$.

Conversely, if $n{+}1$ is an odd prime number and $+2$ generates $\mathbb{Z}_p^\star$, then n is even, and n is the smallest number such that $2^n \equiv 1 \pmod{n{+}1}$, i.e., n is S-prime. □

Example 2.7. (1) If $n = 6$, then $n{+}1$ is prime; but $+2 \notin G_7 = \{-2, +3\}$; hence $6 \notin P(S)$.
(2) Let $n = 12$; then $n{+}1$ is prime, and 12 is S-prime as $+2 \in G_{13} = \{-6, -2, +2, +6\}$. □

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:

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

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

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

Since for odd n, $\overline{S}_n$ 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 [22]. Sequence numbers in [22] which we provide with a star refer to sequences which have been added recently as being new.

Example 2.8. For $n = 8$, we have $\overline{S}(\alpha_8) = a_4a_8a_3a_7a_2a_6a_1a_5$, $\overline{S}_8 = (1\,7\,4)(2\,5\,8)(3)(6)$, $\#\langle \overline{S}_8 \rangle = 3$, and $8 \notin P(\overline{S})$. Remark that $\overline{S}_6 = (1\,5\,4\,6\,2\,3)$, $\#\langle \overline{S}_6 \rangle = 6$ 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 2.9.
(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 2.10. *If n is an $\overline{S}$-prime, then $n+1$ is a prime number.* □

Theorem 2.11. *A number n is $\overline{S}$-prime if and only if $n{+}1$ is an odd prime number and -2 generates $\mathbb{Z}_{n+1}^\star$.* □

Comparing Theorems 2.11 and 2.6 explains why we call the permuting operation $\overline{S}$ dual to S; see also Section 6.

Example 2.12. (1) For $n = 10$, the number $n{+}1$ is prime; but $10 \notin P(\overline{S})$ since $-2 \notin G_{11} = \{-5, -4, -3, +2\}$.
(2) Consider $n = 6$; then $n{+}1$ is prime, and $-2 \in G_7 = \{-2, +3\}$; therefore $6 \notin P(\overline{S})$. □

3 The Twist Operation and Its Primes

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 $T_\bullet$ defined by $T_\bullet(\alpha_n) = a_1a_na_2a_{n-1}a_3a_{n-2}\ \cdots$.

Again we have that the position of the first symbol a_1 of α_n is not changed under $T_\bullet$ and therefore $P(T_\bullet) = \varnothing$. As in the previous section we modify $T_\bullet$ to T by interchanging the two halves of the card deck before shuffling, i.e., T is defined by

$T(\alpha_n) = a_na_1a_{n-1}a_2a_{n-2}a_3\cdots$.

This modified operation T induces permutations T_n with

$T_n(m) = 2m$ if $1 \le m < k = \lceil (n+1)/2 \rceil$, and
$T_n(m) = 2(n-m)+1$ if $k \le m \le n$.

Example 3.1. For α_6 and α_7, we obtain $T(\alpha_6) = a_6a_1a_5a_2a_4a_3$, $T_6 = (1\,2\,4\,5\,3\,6)$, $6 \in P(T)$, $T(\alpha_7) = a_7a_1a_6a_2a_5a_3a_4$, $T_7 = (1\,2\,4\,7)(3\,6)(5)$, and $7 \notin P(T)$. □

For $P(T)$ we have:

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

The elements of $P(T)$ coincide with the so-called Queneau numbers [7]; cf. the sequence A054639 in [22]. 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 T_n^{-1} induced by T^{-1} is defined as follows; cf. [7, 8].

$T_n^{-1}(m) = m/2$ if m is even, and
$T_n^{-1}(m) = n-(m-1)/2$ if m is odd.

The twist operation is a major tool in characterizing the behavior of some types of reversal-bounded multipushdown acceptors [15, 16]. But there is a much earlier interest in $P(T)$ or rather in $P(T^{-1})$: T_n^{-1} plays an important role in generalizations of a certain verse form called *sextine* or *sestina* in Italian [19, 20, 8, 9]. The original sextine is based on T_6^{-1} and consists of six stanzas of six lines each; remember that 6 belongs to the set $P(T^{-1})$.

Crucial in our approach is the fact that the permutation T_n can also be written as

$T_n(m) \equiv +2m \pmod{2n+1}$ if $1 \le m < k = \lceil (n+1)/2 \rceil$, and
$T_n(m) \equiv -2m \pmod{2n+1}$ if $k \le m \le n$.

Then the T-counterpart of Propositions 2.2(1) and 2.9(1) reads as follows.

Proposition 3.2. *If n in $\mathbb{N}_2$ is T-prime, then for each m $(1 \le m < 2n+1)$:*

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

(1) If $n = 4k+1$ $(k \ge 1)$, then we have in this sequence of length n in total: $2k$ multiplications by $+2$ (viz. in case we apply T_n to a number strictly less than $\lceil (n+1)/2 \rceil$) and $2k+1$ multiplications by -2 (viz. when we apply 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 $m \cdot 2^n \equiv -m \cdot 2^{2k} \cdot (-2)^{2k+1} \equiv -m$ (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 3.2. It turns out that if $n \equiv 0 \,(\mathrm{mod}\ 4)$, then n is not T-prime; see [7] or Theorem 3.10 below.

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 3.3. [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 $\mathbb{Z}^{\star}_{2n+1}$, then n is T-prime.*

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

(4) *If $n = 2p$ 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.* □

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[1], as follows.

Theorem 3.4. [8] *A number n in $\mathbb{N}_2$ is T-prime if and only if $2n{+}1$ is a prime number, and at least one of -2 and $+2$ is a generator of $\mathbb{Z}^{\star}_{2n+1}$.* □

Reference [9], which does refer to [7] but not to [8], includes two characterizations of $P(T^{-1})$ (viz. Theorem 2 and Corollary 1 in [9]). Phrased in terms of T-primes we have

Theorem 3.5. [9] *If $n \in \mathbb{N}$ and $p = 2n{+}1$, then*

(1) *n is T-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*

(2) *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 $2 \,(\mathrm{mod}\ 4)$, or 2 is of order n in $\mathbb{Z}/p\mathbb{Z}$ and $n \equiv 3 \,(\mathrm{mod}\ 4)$.* □

The remaining part of this section is devoted to an alternative, more refined, characterization of T-primes (Theorem 3.12 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, T_n and $P(T)$ rather than using T^{-1}, T_n^{-1} and $P(T^{-1})$.

The first step is Lemma 3.6 which has originally been conjectured by R. Queneau[19, 20]; this lemma and Proposition 3.7 have been proven in [8]. We include the proofs because they are useful in other situations as well; see Sections 5 and 6.

Lemma 3.6. [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

[1] In [8] the second condition reads: "either $+2$ or -2 is a generator of $\mathbb{Z}^{\star}_{2n+1}$.". If "either $\cdots$ or $\cdots$" stands for the *exclusive or*, then this version of the result is definitely wrong; cf. our characterization in Theorem 3.12 and Section 4 below.

the permutation 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,

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

So every multiple of $2x+1$ is mapped by T_n on another multiple of $2x+1$. For n to be T-prime, T_n must consists of a single cycle of length n, which implies that all 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 3.7. [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 we need some terminology from number theory.

Definition 3.8. 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 3.9. *$+2$ is a quadratic residue of primes of the form $8k \pm 1$ and a quadratic non-residue of primes of the form $8k \pm 3$. -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 $8k+7$.* □

For a proof of the first half, we refer to Theorem 95 in [12], Theorem 3.103 in [1], or §4.1 in [18]. The second half can be established as Theorem 95 in [12]; cf. Example 4.1.18 in [18].

We now turn to a result from [7] —viz. the third part of Theorem 3.3(5)— and its proof: here it plays a more important role than in [7].

Theorem 3.10. [7] *Let n be a number in $\mathbb{N}_2$. If $n \equiv 0 \pmod{4}$, then n is not T-prime.*

Proof. Assume to the contrary that n, with $n = 4k$ for some $k \geq 1$, is T-prime. Then Proposition 3.7 implies that $2n+1 = 8k+1$ is a prime number p. By Proposition 3.9, the number $+2$ is a quadratic residue of p; so there exists an x with $x^2 \equiv 2 \pmod{p}$.

However, for each x we have $x^{2n} \equiv 1 \pmod{p}$, and so $2^{4k} \equiv 2^n \equiv x^{2n} \equiv 1 \pmod{p}$. Then $(2^{2k}+1)(2^k+1)(2^k-1) \equiv 0 \pmod{p}$ holds, which implies that $2^{2k} \equiv -1 \pmod{p}$ or $2^k \equiv -1 \pmod{p}$ or $2^k \equiv 1 \pmod{p}$. In each of these three cases we have that the absolute value of $T_n^t(2)$ equals 1 where t is equal to $2k-1$, $k-1$ and $k-1$, respectively. Then $T_n^{2t+1}(2) = 2$, 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; cf. [7] for details.

We define for T_n a corresponding permutation q_n which uses $\mathbb{A}_n$ instead of $\mathbb{Z}_{2n+1}$:

$$\begin{aligned} q_n(m) &\stackrel{\circ}{=} 2m && \text{if } 1 \leq m < k = \lceil (n+1)/2 \rceil, \text{ and} \\ q_n(m) &\stackrel{\circ}{=} |2m| && \text{if } k \leq m \leq n. \end{aligned}$$

We use the $\stackrel{\circ}{=}$-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, $q_n(m) \stackrel{\circ}{=} |2m|$ and, more generally, $q_n^t(m) \stackrel{\circ}{=} |2^t m|$ for $1 \leq m \leq n$ and $t \geq 1$.

Example 3.11. If $n = 5$ and we apply 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 $q_5 = T_5$. 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 $q_5^4 = T_5^{-1}$. □

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

Theorem 3.12. *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 $\mathbb{Z}^\star_{2n+1}$ but -2 is not.*

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

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

Proof. Suppose n in $\mathbb{N}_2$ is T-prime. By Proposition 3.7 the number $p = 2n+1$ is an odd prime number and hence $\mathbb{Z}^\star_{2n+1}$, 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 $x^{2n} \equiv 1 \pmod p$.

From Theorem 3.10 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 $n \geq 2$. The second alternative implies that $g^n \equiv 1 \pmod p$ as well, which contradicts Proposition 3.2 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 $k \geq 1$. By Proposition 3.9, -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 3.2(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 $k \geq 0$. Now Proposition 3.9 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 3.2(3) with $m = 1$), and that $+2$ does not generate $\mathbb{Z}^\star_{2n+1}$.

Conversely, if $2n+1$ is a prime number, then $\mathbb{Z}^\star_{2n+1}$ possesses $2n$ elements. Let g be equal to $+2$, -2 or $+2$, and -2, respectively, and consider g^1, g^2, ... , g^{n-1}, g^n, g^{n+1}, ... , g^{2n} in $\mathbb{A}_n$. Since g generates $\mathbb{Z}^\star_{2n+1}$ all these elements in the sequence are different and $g^{2n} \stackrel{\circ}{=} +1$. As $q_n^t(m) \stackrel{\circ}{=} |2^t m|$ for each m $(1 \leq m \leq n)$, the absolute values of the first n elements in this sequence coincide with the sequence $q_n^1(1)$, $q_n^2(1)$, ... , $q_n^n(1)$. Now $q_n^n(1) \stackrel{\circ}{=} 1$, which implies that $|g^n| \stackrel{\circ}{=} 1$; so we have either $g^n \stackrel{\circ}{=} +1$ or $g^n \stackrel{\circ}{=} -1$. But $g^n \stackrel{\circ}{=} +1$ is impossible, as it would mean that $\mathbb{Z}^\star_{2n+1}$ possesses at most n elements instead of $2n$. Hence we have that $g^n \stackrel{\circ}{=} -1$.

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 $q_n^i(1) \stackrel{\circ}{=} q_n^j(1)$ or, equivalently, $g^i \stackrel{\circ}{=} -g^j$ in $\mathbb{A}_n$. As $g^n \stackrel{\circ}{=} -1$ we then obtain that $g^{n+i} \stackrel{\circ}{=} g^j$ in $\mathbb{A}_n$ with $j < n + i$, which contradicts the fact that g generates $\mathbb{Z}^\star_{2n+1}$. Consequently, $\#\langle T_n \rangle = \#\langle q_n \rangle = n$, i.e., n is T-prime. □

Example 3.13. (1) The number 8 is not T-prime; although 17 is a prime number, both $+2$ and -2 fail to belong to $G_{17} = \{-7, -6, -5, -3, +3, +5, +6, +7\}$.

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

(3) In case $n = 6$, we have that $G_{13} = \{-6, -2, +2, +6\}$, which includes both $+2$ and -2, and so 6 is T-prime.

(4) Finally, $3 \in P(T)$ as both 7 is a prime number and -2 is in $G_7 = \{-2, +3\}$. □

Now Theorem 3.4 (the main result from [8]) is a corollary of Theorem 3.12. And some main results from [7] also follow from our characterization of T-primes: cf. Theorem 3.3(1), 3.3(2) and the third part of 3.3(5). Notice that the first part of Theorem 3.3(5) is a consequence of its third part; cf. Theorem 3.12. J.-G. Dumas showed that it is possible to derive his characterization (Theorem 3.5) from Theorem 3.12 and vice versa [10].

4 Operations Based on Archimedes Spiral and Their Primes

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 $r = c\,\theta$ ($c > 0$; $\theta \geq 0$ is the angle). 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. Reading the symbols placed on the X-axis from left to right yields $A_0(\alpha_n)$:

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

The corresponding permutations $A_{0,n}$ satisfy

$$A_{0,n}(m) = \lceil (n+1)/2 \rceil + (-1)^{m-1} \lceil (m-1)/2 \rceil, \qquad 1 \leq m \leq n.$$

It is easy to show that 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 [22].

Example 4.1. Clearly, $A_0(\alpha_5) = a_4 a_2 a_1 a_3 a_5$, $A_{0,5} = (1\,3\,4)(2)(5)$, $\#\langle A_{0,5} \rangle = 3$, and $5 \notin P(A_0)$. Similarly, $A_0(\alpha_6) = a_6 a_4 a_2 a_1 a_3 a_5$, $A_{0,6} = (1\,4\,2\,3\,5\,6)$, 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

$A_1(\alpha_n) = a_{n-1} a_{n-3} \cdots a_3 a_1 a_2 a_4 \cdots a_{n-2} a_n$ if n is even, and
$A_1(\alpha_n) = a_n a_{n-2} \cdots a_3 a_1 a_2 a_4 \cdots a_{n-3} a_{n-1}$ if n is odd,

and for the permutations $A_{1,n}$ induced by A_1

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

For $P(A_1)$ we have that even numbers and the numbers $6k+1$ ($k \geq 1$) are not A_1-prime:

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

cf. sequence A163778* in [22].

Example 4.2. Now we have $A_1(\alpha_5) = a_5 a_3 a_1 a_2 a_4$, $A_{1,5} = (1\,3\,2\,4\,5)$, and $5 \in P(A_1)$; $A_1(\alpha_6) = a_5 a_3 a_1 a_2 a_4 a_6$, $A_{1,6} = (1\,3\,2\,4\,5)(6)$, $\#\langle A_{1,6} \rangle = 5$, and $6 \notin P(A_1)$. □

Remark that with respect to their cycle structure representation we have $A_{0,n} = A_{0,n-1}(n)$ when n is odd, and similarly $A_{1,n} = A_{1,n-1}(n)$ 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. Consider the permuting operation $\rho^{-1}T^{-1}\rho$ where ρ is the reversal operation of Example 1.1. Then we have for even $n \geq 2$, respectively, for odd $n \geq 3$,

$\rho^{-1}T^{-1}\rho(\alpha_n) = \rho T^{-1}\rho(\alpha_n) = \rho T^{-1}(a_n a_{n-1} \cdots a_2 a_1)$
$= \rho(a_{n-1}a_{n-3} \cdots a_3 a_1 a_2 a_4 \cdots a_{n-2}a_n) = a_n a_{n-2} \cdots a_4 a_2 a_1 a_3 \cdots a_{n-3}a_{n-1} = A_0(\alpha_n)$,
$\rho^{-1}T^{-1}\rho(\alpha_n) = \rho T^{-1}\rho(\alpha_n) = \rho T^{-1}(a_n a_{n-1} \cdots a_2 a_1)$
$= \rho(a_{n-1}a_{n-3} \cdots a_4 a_2 a_1 a_3 \cdots a_{n-2}a_n) = a_n a_{n-2} \cdots a_3 a_1 a_2 a_4 \cdots a_{n-3}a_{n-1} = A_1(\alpha_n)$.

These equalities imply that $\#\langle A_{0,n}\rangle = \#\langle \rho_n^{-1}T_n^{-1}\rho_n\rangle = \#\langle T_n^{-1}\rangle = \#\langle T_n\rangle$ for even $n \geq 2$, and $\#\langle A_{1,n}\rangle = \#\langle \rho_n^{-1}T_n^{-1}\rho_n\rangle = \#\langle T_n^{-1}\rangle = \#\langle T_n\rangle$ for odd $n \geq 3$. From these observations the statements follow. □

Combining Theorems 4.3 and 3.12 yields characterizations of $P(A_0)$ and of $P(A_1)$.

Theorem 4.4.
(1) *A number n in $\mathbb{N}_2$ is A_0-prime if and only if n is even, $2n{+}1$ is a prime number, and both -2 and $+2$ are a generator of $\mathbb{Z}^\star_{2n+1}$.*
(2) *A number n in $\mathbb{N}_2$ is A_1-prime if and only if n is odd, $2n{+}1$ is a prime number, and only one of -2 and $+2$ is a generator of $\mathbb{Z}^\star_{2n+1}$.* □

Note that by Theorem 3.12 the first condition in Theorem 4.4(1) may be replaced by "$n \equiv 2 \pmod 4$" as well. Theorem 4.4(2) gives rise to the introduction of the following primes.

Definition 4.5. 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 $P(A_1^+)$ and $P(A_1^-)$, we have (cf. A163779* and A163780* in [22]) respectively

$P(A_1^+) = \{5,\ 9,\ 29,\ 33,\ 41,\ 53,\ 65,\ 69,\ 81,\ 89,\ 105,\ 113,\ 173,\ 189,\ 209,\ 221,\ 233,\ 245,$
$261,\ 273,\ 281,\ 293,\ 309,\ 329,\ 393,\ 413,\ 429,\ 441,\ 453,\ 473,\ 509,\ \ldots\}$;
$P(A_1^-) = \{3,\ 11,\ 23,\ 35,\ 39,\ 51,\ 83,\ 95,\ 99,\ 119,\ 131,\ 135,\ 155,\ 179,\ 183,\ 191,\ 231,\ 239,$
$243,\ 251,\ 299,\ 303,\ 323,\ 359,\ 371,\ 375,\ 411,\ 419,\ 431,\ 443,\ 483,\ 491,\ \ldots\}$.

Theorems 3.12 and 4.4(2) imply the following characterizations of A_1^+- and A_1^--primes.

Theorem 4.6.
(1) *A number n in $\mathbb{N}_2$ is A_1^+-prime if and only if $n \equiv 1 \pmod 4$, $2n{+}1$ is a prime number, and $+2$ is a generator of $\mathbb{Z}^\star_{2n+1}$, but -2 is not.*
(2) *A number n in $\mathbb{N}_2$ is A_1^--prime if and only if $n \equiv 3 \pmod 4$, $2n{+}1$ is a prime number, and -2 is a generator of $\mathbb{Z}^\star_{2n+1}$, but $+2$ is not.* □

For a permuting operation X, we define the set $H(X)$ by $H(X) = \{n/2 \mid n \in P(X) - \{2\}\}$. Now we are able to relate the shuffle primes of Section 2 to the T- and Archimedes primes.

Theorem 4.7.
(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) If $n \in H(S)$, then $n \geq 2$, $2n \in P(S)$, $2n{+}1$ is an odd prime (Proposition 2.5), and $2 \in G_{2n+1}$ (Theorem 2.6). Theorems 3.12, 4.4(1), and 4.6 imply that $n \in P(A_0) \cup P(A_1^+)$.

Conversely, if $n \in P(A_0) \cup P(A_1^+)$, then $2n{+}1$ is prime and $+2$ generates $\mathbb{Z}^\star_{2n+1}$ (Theorems 4.4 and 4.6). Then by Theorem 2.6 we have $2n \in P(S)$ and, consequently, $n \in H(S)$.

(2) The proof is similar: we use Proposition 2.10 and Theorem 2.11 instead of Proposition 2.5 and Theorem 2.6, respectively. □

From Theorems 4.4(1), 4.6, 4.7 and the fact that $P(A_0)$, $P(A_1^+)$ and $P(A_1^-)$ are mutually disjoint sets, we infer the following two characterizations.

Corollary 4.8. *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* $\mathbb{Z}^\star_{2n+1}$, *but* -2 *does not.*
(2) $n \equiv 2 \pmod 4$ *and both* -2 *and* $+2$ *generate* $\mathbb{Z}^\star_{2n+1}$. □

Corollary 4.9. *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* $\mathbb{Z}^\star_{2n+1}$.
(2) $n \equiv 3 \pmod 4$, -2 *generates* $\mathbb{Z}^\star_{2n+1}$, *but* $+2$ *does not.* □

5 Operations Based on the Josephus Problem and Their Primes

This section is devoted to an infinite sequence of permuting operations on strings, denoted by $\{J_k\}_{k\geq 2}$, which are related to the so-called (Flavius) Josephus problem; cf. §1.3 in [11] and §3.4 in [13]. For an excellent introduction, including many historical details, we refer to [21].

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.

We have $P(J_1) = P(\lambda) = \varnothing$ as J_1 is equal to the identity operation λ (Example 1.1).

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

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

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 [13]. The corresponding 19 sequences in [22] are A163782* — A163800*, respectively.

Example 5.2. We already saw that $J_2(\alpha_5) = a_2a_4a_1a_5a_3$. Then $J_{2,5} = (1\,3\,5\,4\,2)$, and consequently 5 belongs to $P(J_2)$. 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 $J_{2,14} = (1\ 11\ 10\ 5\ 13\ 14\ 7\ 9\ 12\ 6\ 3\ 8\ 4\ 2)$. □

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

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 $2 \leq n \leq 1000000$ $(3 \leq k \leq 20)$.

In §3.3 of [11] 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 $J_{k,n}^{-1}(n)$ has been computed in [11]. However, this approach can be extended to obtain all values of $J_{k,n}^{-1}$ and, in addition, to derive closed forms for $J_{2,n}^{-1}$ and $J_{2,n}$. This latter achievement is exceptional since looking for a closed form for $J_{k,n}^{-1}$ or $J_{k,n}$ with $k \geq 3$ seems to be difficult; cf. §3.3 in [11].

The idea of this method is very simple. We walk in a cyclic way through the standard word α_n and we assign numbers 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 case $J_{2,n}$, 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 $J_{2,14}$ 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 13th place, and 13 in the 14th 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 marking process, we want to determine which symbol a_j arrives at position $N/2$ in the permutation $J_{2,n}$, i.e, we want to determine the number j that satisfies $J_{2,n}(j) = N/2$ or, equivalently, we want to compute $J_{2,n}^{-1}(N/2)$. 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 §3.3 of [11] this iteration process is captured in an algorithm to determine the value of $J_{3,n}^{-1}(n)$. This algorithm can easily be generalized —viz. to compute all values $J_{3,n}^{-1}(m)$— and simplified, since starting with J_2 instead of J_3 means a considerable reduction in structural complexity. The modified algorithm for computing $J_{2,n}^{-1}(m)$ with $1 \leq m \leq n$, reads as follows.

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

As in §3.3 of [11] we transform the above algorithm in an even simpler one:

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

Example 5.4. Applying these algorithms with $n = 14$ and $m = 4$ results, after skipping the loops, in $J_{2,14}^{-1}(4) = 8$. When we start the first algorithm with $m = 14$, the successive values of N are 28, 27, 25, 21 and 13; thus $J_{2,14}^{-1}(14) = 13$; 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 $J_{2,14}^{-1}(13) = 5$; 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 $L(m, n) = \lceil \lg((n+1)/(2n+1-2m)) \rceil$; we use "lg" to denote the base-2 logarithm as in [11]. Hence

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

This definition of $J_{2,n}^{-1}$ can even be reduced to the closed form

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

or even to

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

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

For even m, it is now easy to define $J_{2,n}$: $J_{2,n}(m) = m/2$ 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 definitions of $J_{2,n}^{-1}$. Fortunately, there is a way out: we can "invert" our two algorithms; inverting the second algorithm results in

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

Example 5.5. If we execute this algorithm with $n = 14$ and $m = 8$, the loop will be skipped, and $J_{2,14}(8) = 4$. For $m = 13$, the algorithm obtains the respective D-values: 16, 8, 4, 2 and 1; hence $J_{2,14}(13) = 14$; cf. Example 5.4. □

From this algorithm we infer that

$$J_{2,n}(m) = (2n + 1 - \llparenthesis 2n + 1 - m \rrparenthesis)/2 \qquad (1 \leq m \leq n),$$

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

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 $n \geq 1$,*

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

Proof. Our argument is based on Exercise 3.34 in [11]. 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 $\lceil \lg((n+1)/(2m-1)) \rceil$ vanishes. Let $k = \lceil \lg \lceil n/2 \rceil \rceil$. Then $2^k \leq n-1$ 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[11]. For instance, $\sum_{m=1}^{n} a_m$ may be written as $\sum a_m (1 \leq m \leq n)$ using this convention. Then we have

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

$$
\begin{aligned}
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} j \left(\left\lceil \frac{n+1+2^{j-1}}{2^j} \right\rceil - \left\lceil \frac{n+1+2^j}{2^{j+1}} \right\rceil \right) \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} j \left(\left\lceil \frac{2n+2+2^j}{2^{j+1}} \right\rceil - \left\lceil \frac{n+1+2^j}{2^{j+1}} \right\rceil \right) \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} \left\lceil \frac{2n+2+2^j}{2^{j+1}} \right\rceil - \lceil \lg(n+1) \rceil \cdot \left\lceil \frac{n+1+2^{\lceil \lg(n+1) \rceil}}{2^{\lceil \lg(n+1) \rceil + 1}} \right\rceil \\
&= \sum_{j=1}^{\lceil \lg(n+1) \rceil} \left\lceil \frac{n+1}{2^j} + \frac{1}{2} \right\rceil - \lceil \lg(n+1) \rceil \; = \sum_{j=1}^{\lceil \lg(n+1) \rceil} \left\lceil \frac{n+1}{2^j} - \frac{1}{2} \right\rceil .
\end{aligned}
$$

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" [11], 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., $\lceil (n+1)/2^j - 1/2 \rceil = \lceil ((n-1)+1)/2^j - 1/2 \rceil$; cf. Exercise 3.22 in [11]. The only exception is when $j = 1 + \lg(n/\lfloor\!\lfloor n \rfloor\!\rfloor)$ where $\lfloor\!\lfloor n \rfloor\!\rfloor$ is again the odd integer such that $n/\lfloor\!\lfloor n \rfloor\!\rfloor$ is a power of 2. In this exceptional case we have $\lceil (n+1)/2^j - 1/2 \rceil = 1 + \lceil ((n-1)+1)/2^j - 1/2 \rceil$, 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 [11], 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 $J_{2,n}^{-1}$ 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 $J_{2,n}^{-1}$ is much more convenient than applying $J_{2,n}$. 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 3.2:

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. Applying $J_{2,n}^{-1}$ iteratively n times to m results in all values 1, 2, ... , n in some order and $(J_{2,n}^{-1})^n(m) = m$, as n is J_2^{-1}-prime. By Lemma 5.6, we obtain

$$\begin{aligned}(J_{2,n}^{-1})^n(m) &\equiv 2^n \cdot m \cdot \textstyle\prod_{j=1}^{n} 2^{\left\lceil \lg \frac{n+1}{2n+1-2j} \right\rceil} \equiv 2^n \cdot m \cdot 2^{\sum_{j=1}^{n} \left\lceil \lg \frac{n+1}{2n+1-2j} \right\rceil} \pmod{2n{+}1} \\ &\equiv 2^n \cdot m \cdot 2^{\sum_{j=1}^{n} \left\lceil \lg \frac{n+1}{2j-1} \right\rceil} \equiv m \cdot 2^{2n} \equiv m \pmod{2n{+}1}.\end{aligned}$$

This implies $2^{2n} \equiv 1 \pmod{2n{+}1}$. As in the proof of Proposition 2.2(1) —except for now using $2n$ instead of n— we obtain that $m \cdot 2^n \equiv -m \pmod{2n{+}1}$.

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

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

The closed form for $J_{2,n}^{-1}$ yields J_2-counterparts of Lemma 3.6 and Proposition 3.7.

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 3.6 slightly: we only need to show that $J_{2,n}^{-1}$ 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

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

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

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 3.7 except that we use Lemma 5.9 instead of Lemma 3.6. □

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

Proof. In both cases the arguments are very similar to the one of Theorem 3.10.

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 3.9). 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 3.10. □

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 $\mathbb{Z}^\star_{2n+1}$, but -2 does not.*
(2) $n \equiv 2 \pmod 4$ *and both -2 and $+2$ generate $\mathbb{Z}^\star_{2n+1}$.*

Proof. Using Propositions 5.8 and 5.10 (instead of Propositions 3.2 and 3.7) and Theorem 5.11 (instead of Theorem 3.10) the proof is analogous to the one of Theorem 3.12. □

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, however, to be a member of the set $G_{43} = \{-17, -15, -14, -13, -10, -9, 3, 5, 12, 18, 19, 20\}$.
(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 3.13(2).
(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 3.14(3). □

The characterization of J_2-primes in Theorem 5.12 can, of course, be related to the main resluts of Section 4; cf. Theorems 4.4(1), 4.6(1) and 5.12 and, respectively, 4.7(1) and 5.14.

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: $P(J_2) = P(A_0) \cup P(A_1^+)$.* □

Corollary 5.15. $P(J_2) = H(S)$. □

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 $g_{i,1}, \ldots, g_{i,M(i)} \in G_{\gamma(n)}$, ($M(i) \ge 1$), but $h_{i,1}, \ldots, h_{i,N(i)} \notin G_{\gamma(n)}$, ($N(i) \ge 0$)",
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 ($1 \le i \le K$):
(*i*) $Q_i(n)$ and $-g_{i,1}, \ldots, -g_{i,M(i)} \in G_{\gamma(n)}$, but $-h_{i,1}, \ldots, -h_{i,N(i)} \notin G_{\gamma(n)}$",
where the Q_i's are mutually exclusive predicates, and there exists a bijection

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

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 dual to S: $K = 1$, $\gamma(n) = n+1$, $M(1) = 1$, $N(1) = 0$ and $g_{1,1} = +2$; cf. Theorems 2.6 and 2.11. Note that S is dual to $\overline{S}$ as well.
(2) According to Theorem 4.6, 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 general problems: the *existence problem* (Given a permuting operation X, does there exists a permuting operation $\overline{X}$ that is dual to X?) and the *unicity problem* (Given permuting operations X and $\overline{X}$ such that $\overline{X}$ is dual to X, is $\overline{X}$ unique?).

Remark that for the more interesting permuting operations considered so far, with the exception of J_2, we have solved the existence problem[2].

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

$\overline{T_n}(m) = n + 2 - 2m$ if $1 \leq m \leq k = \lceil n/2 \rceil$, and
$\overline{T_n}(m) = 2(m-k) - d$ if $k < m \leq n$;

where $d = 1$ if n is even and $d = 0$ if n is odd; cf. [6].

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

$\overline{J_{2,n}}^{-1}(m) \equiv -2m \pmod{2n+1}$ 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 §3.3 of [11]; 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 and odd (numbered) sweeps through α_n:

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

As in §3.3 of [11] the even numbers in the numbering/marking process determine the value of $\overline{J_{2,n}}(m)$: the jth symbol to be marked receives number $2j$ in the marking process.

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

Example 6.3. We apply this numbering process to $\overline{J_{2,14}}$. 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 $\overline{J_{2,14}} = (1\ 4\ 6\ 10\ 9\ 11\ 7\ 2\ 8\ 13\ 3\ 12\ 5\ 14)$, $\#\langle \overline{J_{2,14}} \rangle = 14$ and $14 \in P(\overline{J_2})$. □

[2]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.

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

$N := 2 * m$;
while $N \leq n$ **do** $N := 2 * n + 1 - 2 * N$;
$\overline{J_{2,n}}^{-1}(m) := 2 * n + 1 - N$

and, respectively, (using the binary mod-operation; cf. [11])

$D := 2 * n + 1 - 2 * m$;
while $D > n$ **do** $D := (-2 * D) \bmod (2 * n + 1)$;
$\overline{J_{2,n}}^{-1}(m) := D$.

Example 6.4. If $n = 14$ and $m = 11$, then $N = 22$ and $D = 7$, the loops will be skipped and $\overline{J_{2,14}}^{-1}(11) = 7$. For $m = 5$, the first algorithm yields as successive values of N: 10, 9, 11, 7 and 15; hence $\overline{J_{2,14}}^{-1}(5) = 14$. The second algorithm obtains as D-values: 19, 20, 18, 22 and 14 and it results in $\overline{J_{2,14}}^{-1}(5) = 14$ as well; cf. Example 6.3. □

To derive a mathematical expression for $\overline{J_{2,n}}^{-1}$ from these algorithms is not as straightforward as in the case of $J_{2,n}^{-1}$; when we 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 process to $\overline{J_{2,13}}$ 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. In case $n = 14$ (cf. Example 6.3) we have the following values for $L(m, 14)$:

$\overline{J_{2,14}}(m)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(m, 14)$	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 $u = 4$, $L(m, 14)$ is odd when $1 \leq m \leq 4$ and $L(m, 14)$ 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

$$\begin{array}{l|l} N_1 = p - 4m & N_2 = 8m - p \\ N_3 = 3p - 16m & N_4 = 32m - 5p \\ N_5 = 11p - 64m & N_6 = 128m - 21p \\ N_7 = 43p - 256m & N_8 = 512m - 85p \end{array}$$

where $p = 2n{+}1$. From these values of N_i, it is easy to infer that for $t \geq 0$, $N_{2t+1} = (2 \cdot 4^t + 1)p/3 - 4^{t+1} \cdot m$ and $N_{2t} = 2 \cdot 4^t \cdot m - (4^t - 1)p/3$. From these expressions it follows that $N_{i+2} - N_{i+1} = -2(N_{i+1} - N_i)$, i.e., N_i is the solution of the difference equation $N_{i+2} + N_{i+1} - 2N_i = 0$ with $N_0 = 2m$ 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 $i \geq 0$, $N_i \equiv 2m \cdot (-2)^i \pmod{2n + 1}$. 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 $N_i = ((6m - 2n - 1)(-2)^i + 2n + 1)/3 < 2n + 1$, which implies $2^i > (4n + 2)/(2n + 1 - 6m)$, and so

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

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

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

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

As $\left\lceil \lg \frac{n+2}{6m-2n-1} \right\rceil_E = 0$ for $k \leq m \leq n$, we obtain for $\overline{J_{2,n}}^{-1}$ in case $n \not\equiv 1 \pmod 3$,

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

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

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. Again, we consider the case $n = 14$, i.e., $\overline{J_{2,14}}^{-1}$; 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	$10 \leq m \leq 14$
$L(m, 14)$	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	$-2m$
$\overline{J_{2,14}}^{-1}(m)$	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 $\overline{J_{2,14}}^{-1} = (1\ 14\ 5\ 12\ 3\ 13\ 8\ 2\ 7\ 11\ 9\ 10\ 6\ 4)$. This agrees with the last line in this table. □

As in the Section 5 it is possible to "invert" the two algorithms for $\overline{J_{2,n}}^{-1}$. Inverting the second algorithm yields:

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

Example 6.8. Executing this algorithm with $n = 14$ and $m = 7$, results in $D = 7$: the loop will be skipped and $\overline{J_{2,14}}(7) = 11$. Starting the algorithm with $m = 14$, produces successive D-values: 14, 22, 18, 20 and 19 and we obtain $\overline{J_{2,14}}(14) = 5$; cf. Example 6.4. □

From this algorithm we obtain the following closed form for the permutation $\overline{J_{2,n}}$:

$$\overline{J_{2,n}}(m) = (2n + 1 - [\![m]\!]^-_{2n+1})/2 \qquad (1 \le m \le n),$$

where $[\![x]\!]^-_q$ is the odd number such that $1 \le [\![x]\!]^-_q < q$ and $x \equiv [\![x]\!]^-_q (-2)^t \pmod q$ for the smallest $t \ge 0$. As examples, we mention that $[\![6]\!]^-_{29} = 21$ and $[\![2]\!]^-_{35} = 23$, 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 $1 \le x < q$, we have $[\![x]\!]^-_q = x$ 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 $\overline{J_{2,14}}$; Examples 6.7 and 6.8 may be used to check the results of this computation.

In applications the closed form for $\overline{J_{2,n}}^{-1}$ is much more convenient than the one for $\overline{J_{2,n}}$; 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 $\overline{J_{2,n}}^{-1}$. And, of course, we rely on the equality $P(\overline{J_2}) = P(\overline{J_2}^{-1})$. For the set of $\overline{J_2}$-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 [22] 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 [11], 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 in that case we construct 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 6.12.

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

(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 $x, y \ge 1$ 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 3.6. First, notice that for $n \not\equiv 1 \pmod 3$, the permutation $\overline{J_{2,n}}^{-1}$ may be written as

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

where the $c_{m,n}$ $(1 \le m \le n)$ 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 $\overline{J_{2,n}}^{-1}$ maps multiples of $2x+1$ on multiples of $2x+1$. Then the statement follows as in the proofs of Lemma 3.6 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 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 $n = 4k + 1$ $(k \ge 1)$ 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 3.9). Then again it is straightforward to derive contradictions as in the proofs of Theorems 3.10 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 $\mathbb{Z}^\star_{2n+1}$.*

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

Proof. The argument is almost identical to the proofs of Theorems 3.12 and 5.12. But now we use Propositions 6.10 and 6.12 (instead of Propositions 3.2 and 3.7, respectively 5.8 and 5.10) and Theorem 6.13 (instead of Theorems 3.10, respectively 5.11). □

Example 6.15 (1) When $n = 14$, condition (1) of Theorem 6.14 applies: $-2, +2 \in G_{29} = \{\pm 2, \pm 3, \pm 8, \pm 10, \pm 11, \pm 14\}$ and $14 \in P(\overline{J_2})$. Cf. Examples 6.3 and 6.7.
(2) For $n = 11$, we have $11 \equiv 3 \pmod 4$, 23 is a prime number, and -2 belongs to the set $G_{23} = \{-9, -8, -6, -4, -3, -2, 5, 7, 10, 11\}$; so 11 is $\overline{J_2}$-prime. □

As to be expected, we now can combine Theorem 6.14 with the results of Section 4; cf. Theorems 4.4, 4.9 and 6.14 and, respectively, Theorems 4.10(2) and 6.16.

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: $P(\overline{J_2}) = P(A_0) \cup P(A_1^-)$.* □

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

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

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 structural properties, a phenomenon already suggested in §1.3 of [11][3]. 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 more intersting 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, 4.7, 5.14 and 6.16 as well as Corollaries 5.15 and 6.17. 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, 9].

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 2.6, 2.11, 3.12, 4.4, 4.6, 4.7, 5.12 and 6.14. More on these X-primes (counting X-primes, distribution of X-primes, weak twin X-prime conjectures, etc.) can be found in [6].

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, Permuting operations on strings — Their permutations and their primes (2009), `http://eprints.eemcs.utwente.nl/15655/`, TR-CTIT-09-26; see also P.R.J. Asveld, Some families of permutations and their primes (2009), `http://eprints.eemcs.utwente.nl/15678/`, TR-CTIT-09-27, Dept. of Comp. Sci., Twente University of Technology, Enschede, The Netherlands.
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.

[3]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 [13].

9. J.-G. Dumas, Caractérisation des quenines et leur représentation spirale, *Math. Sci. Humaines/Math. Soc. Sci.* **184** (2008) 9–23.
10. J.-G. Dumas, personal communication (September 4, 2009).
11. R.L. Graham, D.E. Knuth & O. Patashnik, *Concrete Mathematics* (1989), Addison-Wesley, Reading, MA.
12. G.H. Hardy & E.M. Wright, *An Introduction to the Theory of Numbers* (1938), Fourth edition (1959), Oxford University Press, Oxford, UK.
13. I.N. Herstein & I. Kaplansky, *Matters Mathematical* (1974), Harper & Row, New York.
14. M. Jantzen, The power of synchronizing operations on strings, *Theoret. Comput. Sci.* **14** (1981) 127–154.
15. M. Jantzen, Hierarchies of principal twist-closed trios, *STACS* 98, Lect. Notes in Comput. Sci. **1373** (1998) Springer, Berlin, pp. 344–355.
16. M. Jantzen & A. Kurgansky, Refining the hierarchy of blind multicounter languages and twist-closed trios, *Inform. Comput.* **185** (2003) 158–181.
17. M. Lothaire, *Combinatorics on Words* (1983), Addison-Wesley, Reading, MA.
18. R.A. Mollin, *Fundamental Number Theory with Applications* (1998), CRC Press, Boca Raton, FL.
19. R. Queneau, *Bâtons, chiffres et lettres* (1965), Gallimard, Paris.
20. R. Queneau, Note complémentaire sur la sextine, *Subsidia Pathaphysica* Troisième et nouvelle série (1965) No. 1, 79–80.
21. P. Schumer, The Josephus problem; once more around, *Math. Mag.* **75** (2002) 12–17.
22. 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.