Playing with Palindromes

Section 1: Palindromes

Let $A[0\,..\,l-1]$ denote a string of l characters.

A **Palindrome** $A[0\,..\,l-1]$ is a string that reads the same backwards as forwards.

For example, let's take a look at these two strings: HELLO and RADAR

"HELLO" read backwards is "OLLEH". That isn't the same and so it's not a palindrome

"RADAR" backwards is still "RADAR". So, this string is a palindrome.

Definition 1.1. A string $A[0\,..\,l-1]$ is a *palindrome* if

$$A[i] = A[l-i-1] \tag{1}$$

where $A[i]$ refers to the i^{th} character in A $\forall i \in \{0, \ldots, l-1\}$

The indices of the characters that are the same would be $(i,\ l-i-1)$.

Definition 1.2. A pair of indices $\{x, y\}$ are *twins* in a string $A[0\,..\,l-1]$ if

$x + y = l - 1$.

In addition, if $A[x] = A[y]$ then they are *palindromic twins*.

Let's take the string "SLEEPPEELS" of length $l = 10$ which is a palindrome. The palindromic twins are denoted by arcs in **Fig 1.1.**

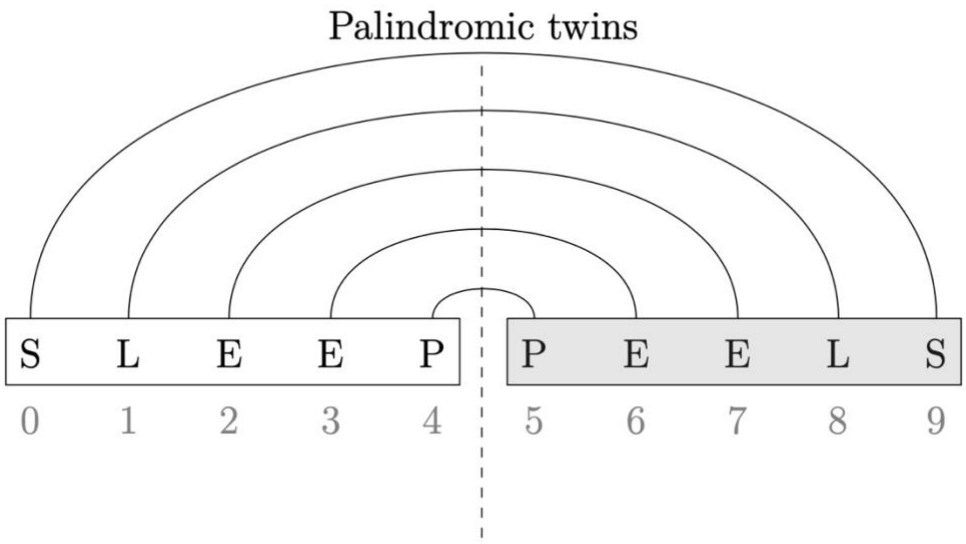


Fig 1.1: Palindromic Twins

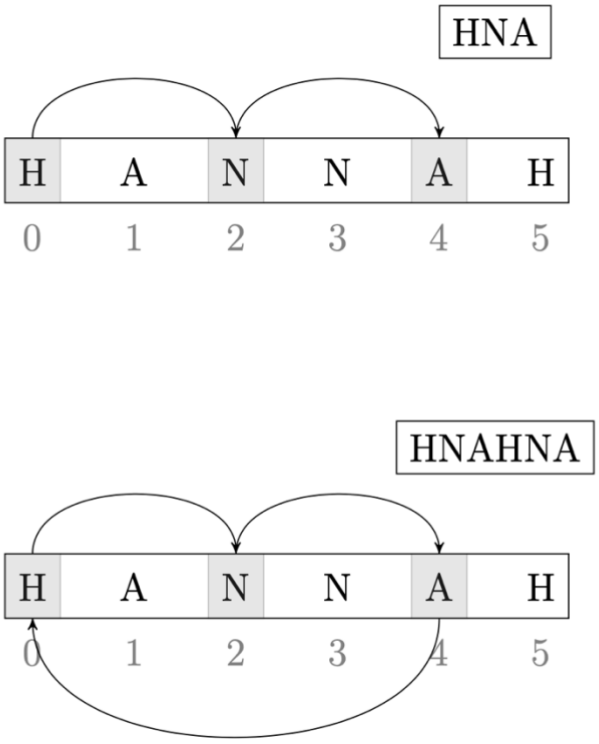
Section 2: Cyclic Shift of a Palindrome

Consider a palindrome $A[0\ ..\ l-1]$. Let's start picking every k^{th} character of A (allowing wrap-around) starting from some starting index s to generate a new string $B[0\ ..\ l-1]$.

We call k as the *cycle length*.

For example, the string "HANNAH" has $l = 6$ and is a palindrome.

Let's start picking every 2^{nd} character of "HANNAH" (cycle length $k = 2$) starting from the beginning of the string ($s = 0$). We get 'H' at index 0, next 'N' at index 2, and then 'A' at index 4. At this point, we've reached the end of the string. To get the next character (as we allow wrapping around) we treat the string as a "circular string" and jump 2 characters. Hence the next character to be picked would be at index 0 which would be 'H' again.



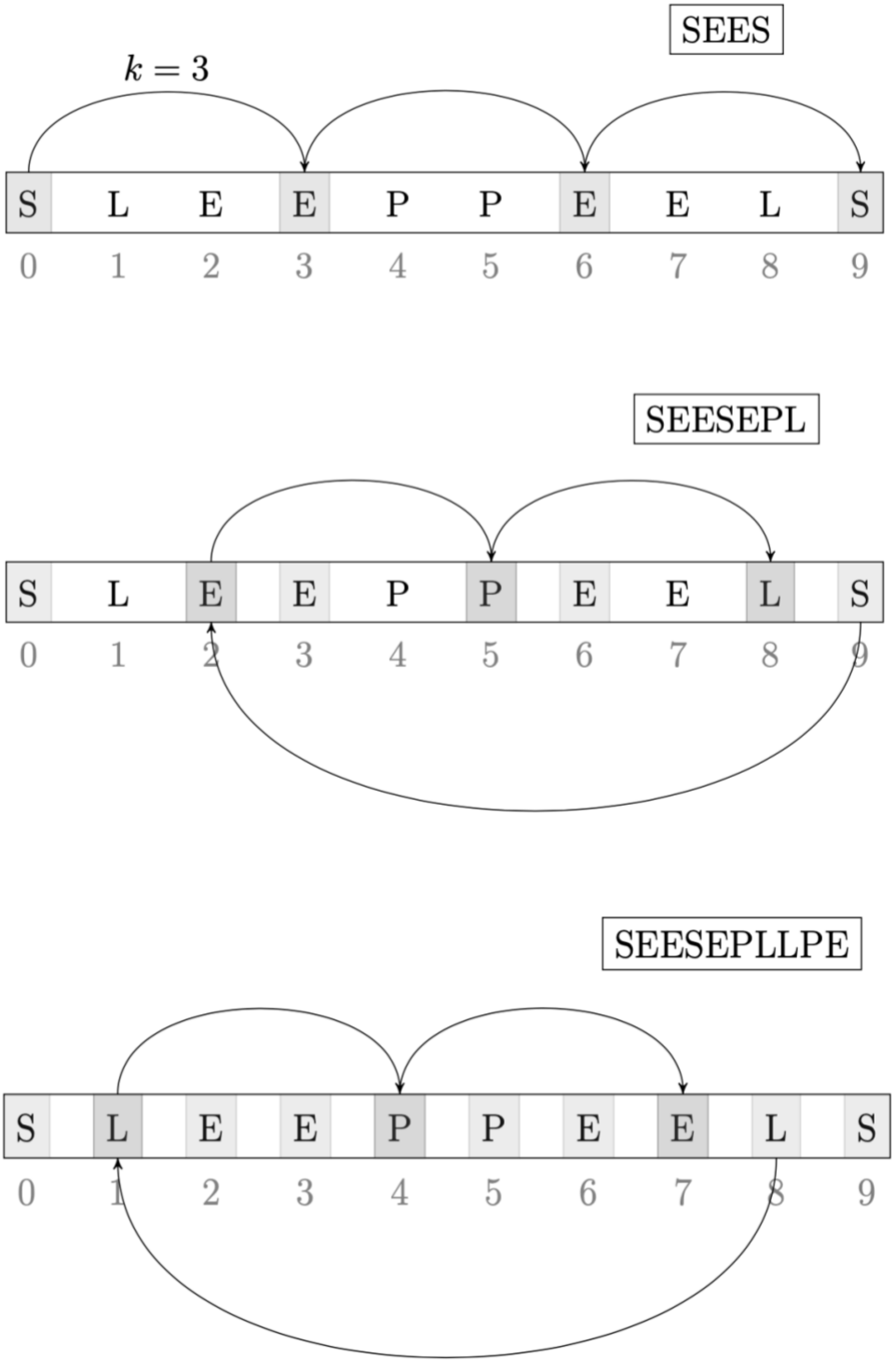
Example 2.1: Picking characters with $k = 2$ in HANNAH.

We stop when we get a new string B that is the same length as our original string A which is 6. So, with cycle length $k = 2$, the new string becomes "HNAHNA".

Now, if k is relatively prime to the length of the string l, then while generating the string B you will always pick a distinct index from string A (no index gets repeated as $\gcd(k, l) = 1$).

Let's take the same string "SLEEPPEELS" (used as an example in Definition 1.2) of length $l = 10$ as A again with $s = 0$.

The cycle lengths that are relatively prime to 10 are: {1,3,7,9}. Let's take $k = 3$ as an example and try to generate B.



Example 2.2: Picking characters with $s = 0$ and $k = 3$ in SLEEPPEELS.

This gives us the string: SEESEPLLPE.

So, if we start from some starting index s and generate a new string $B[0 \,..\, l-1]$, then each index of A is mapped to a distinct index of B.

We call this process as the cyclic shift of the string A with cycle length k and B is the cyclic-shifted string.

But how are these indices getting mapped in B?

If we look at the indices of the above example, we can observe that the cyclic-shifted string B has indices from the original string A in this order:

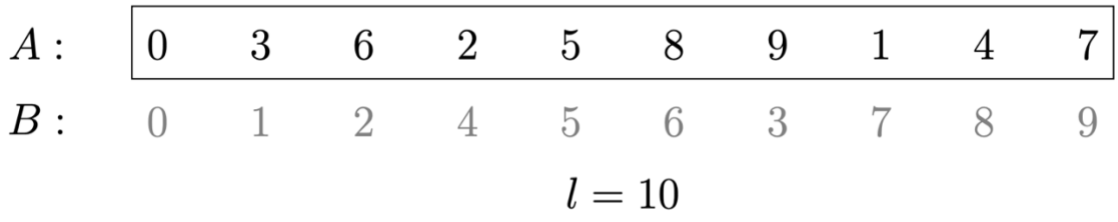


Fig 2.1: Mapped indices of A in B. For example: B[1] = A[3], B[4] = A[2] and so on.

We can observe that these values are equal to $3i \mod 10$ where i is the index in the new string B.

In general, if the cycle length is k and starting index $s = 0$, the i^{th} position of B will have the character

$$A[ki \,\%\, l] \tag{2}$$

We define the above process more formally as follows.

Definition 2.1. Consider a string $A[0 \,..\, l-1]$, a starting index s and a cycle length k that is relatively prime to l. A *cyclic shift* of A denoted by $cyclic(A,\ s,\ k)$ results in a new string B such that $B[i] = A[(s + ki) \,\%\, l]$.

The condition that the cycle length k is relatively prime to l ensures that there is a one-to-one mapping between the indices of A and B.

In particular, if $s = 0$

$$A[ki \ \% \ l] \leftrightarrow B[i] \tag{3}$$

In **Example 2.2**, we saw that $cyclic(SLEEPPEELS,\ 0,\ 3) = SEESEPLLPE = B$

Similarly,

$$\begin{aligned} cyclic(RADAR, 0, 1) &= RADAR \\ cyclic(RADAR, 0, 3) &= RAARD \\ cyclic(RADAR, 2, 3) &= DRAAR \end{aligned} \tag{4}$$

Section 3: Result

Theorem 3.1. Suppose $A[0\ ..\ l-1]$ is a palindrome and a number k is relatively prime to l. Then there exists a starting index s^* such that $cyclic(A, s^*, k)$ results in another palindrome B.

- **Example:** Let's take A to be the string: $abcdefghijjihgfedcba$. Here $l = 20$. Let's take $k = 3$ (as gcd(3,20) $= 1$) and $s^* = 1$.

  $cyclic(A, 1, 3)$ will result in $B = behjgdacfiifcadgjheb$ which is also a palindrome.

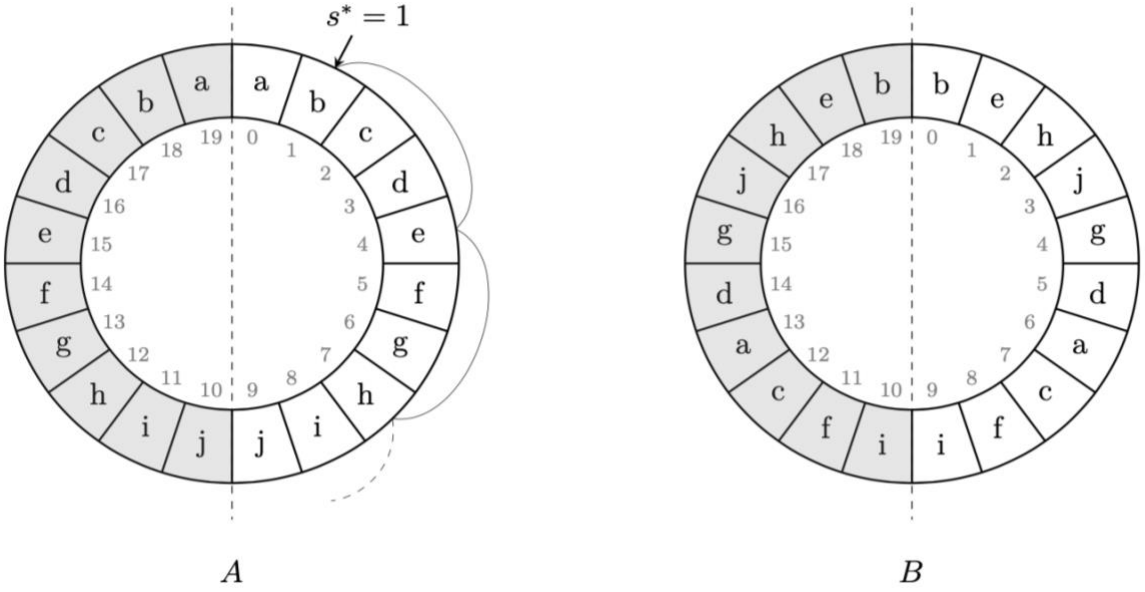


Fig 3.1: Cyclic shift of A with $k = 3$ and $s^* = 1$ gives B.

Let us assume we have a string A of length l. Let A be a palindrome. Suppose we get B by performing a cyclic shift – $cyclic(A, s^*, k)$ on A with the starting position s^* and cycle length k.

The right choice of s* turns out be the solution to $2s^* \equiv (k-1) \mod l$.

We will first prove that s^* is always an integer in **Lemma 3.1**.

Lemma 3.1. Let k and l be positive integers such that $k < l$ and k is relatively prime to l. Then there exists a $s^* \in \{0,1,..,\ l-1\}$ such that $2s^* \equiv (k-1) \mod l$.

Proof.

Case 1: k is odd

Then, $k - 1 = 2t$ for some $t \in [0, l-1]$. So, we can pick $s^* = t$. Therefore, s^* is an integer.

Case 2: k is even

Since, $\gcd(k, l) = 1$, l has to be odd.

Hence, 2 is relatively prime to l.

The set of numbers relatively prime to l form a multiplicative group. [1] [2]

So, every number in this set has an inverse. Hence, 2 also has an inverse.

So, $s^* \equiv 2^{-1}(k-1) \mod l$. Therefore, s^* is an integer.

As 2 is relatively prime to l,

$$\begin{aligned} 2.2^{-1} &\equiv 1 \mod l \\ 2.2^{-1} &\equiv l+1 \mod l \\ 2.2^{-1} &\equiv 1 \mod l \end{aligned} \tag{5}$$

Thus, there exists a $s^* \in \{0,1,..,\ l-1\}$ such that $2s^* \equiv (k-1) \mod l$.

■

Now we will prove that if we take the starting point s = s*, then the cyclic shift of a palindrome will result in another palindrome.

Let u and v be indices in A that get mapped to indices x and y in B, respectively under $cyclic(A, s^*, k)$.

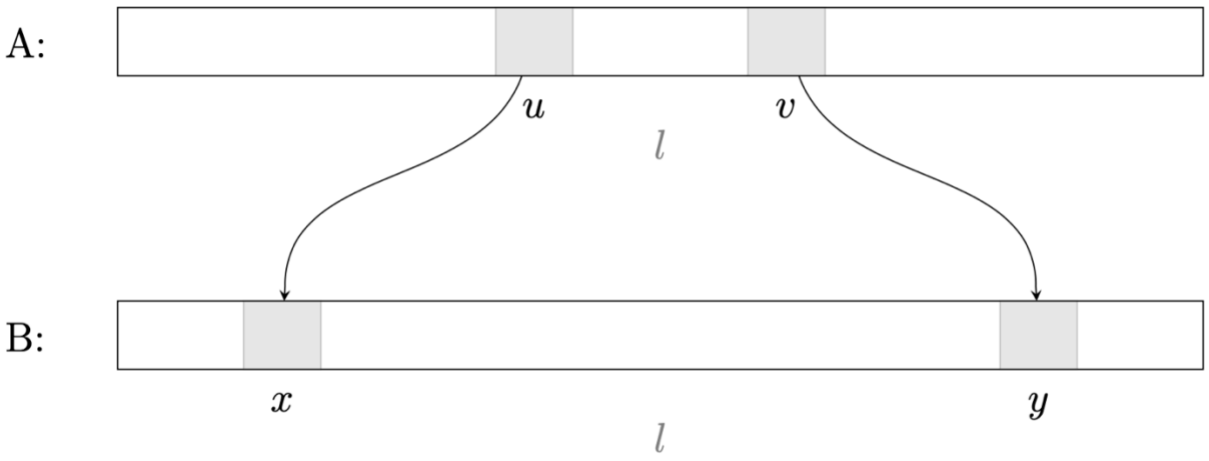


Fig 3.2: Cyclic Shift of *A* resulting in *B* where $\{x, y\}$ is assumed to be a twin.

We show that $B[x] = B[y]$ if $\{x, y\}$ is a twin. This suffices to show that B is a palindrome.

Lemma 3.2. If $x + y = l - 1$, then $B[x] = B[y]$.

Proof.

From our discussion earlier in **Definition 2.1**,

$$u \equiv (s^* + kx) \mod l \tag{6}$$

$$v \equiv (s^* + ky) \mod l \tag{7}$$

Adding equations (6) and (7) we get,

$$\begin{aligned} u+v &\equiv 2s^* + k(x+y) \bmod l \\ u+v &\equiv 2s^* + k(l-1) \bmod l \ \ [\text{as } x+y = l-1] \\ u+v &\equiv k-1+k(l-1) \bmod l \ \ [\text{as } 2s^* \equiv (k-1) \bmod l] \\ u+v &\equiv k-1+kl-k \bmod l \\ u+v &\equiv -1 \bmod l \\ u+v &\equiv l-1 \bmod l \end{aligned}$$

Hence,

$$u + v = l - 1 \tag{8}$$

Therefore, u and v are palindromic twins in A. We know that $A[u] = A[v]$ since A is a palindrome. Since, the indices u and v are mapped to indices x and y respectively in B, we have

$$B[x] = A[u] = A[v] = B[y] \tag{9}$$

Thus,

$$B[x] = B[y] \tag{10}$$

For any pair of twins $\{x, y\}$ in B, equation (10) holds. Hence B is a palindrome.

■

Proof of Theorem 3.1.

We have shown that there is always an index s^* in A satisfying the equation

$2s^* \equiv (k-1) \bmod l$. (**Lemma 4.1**)

We have also shown that a cyclic shift of a palindrom A under such a s^* will also result in a palindrome B. (**Lemma 4.2**)

Hence, it follows that there exists a starting index s^* in a palindrome A such that $cyclic(A, s^*, k)$ results in another palindrome B when k is relatively prime to l.

In fact, s^* has an explicit formula as given below:

$$s^* = \begin{cases} \dfrac{k-1}{2} & \text{if } k \text{ is odd} \\ \dfrac{(l+1)(k-1)}{2} \bmod l & \text{otherwise} \end{cases}$$

■

Section 4: Remarks

Another way to view our result is that a circular palindrome will get mapped to another circular palindrome, no matter where we start. However, if you start at a $s \neq s^*$ then the axis of symmetry gets rotated by R indices. For a given l and k, can we calculate the value for R?

For example, let's consider the same string $abcdefghijjihgfedcba$ as A. Now, performing $cyclic(A, 0,3)$ will result in the string $B = adgjhebbehjgdacfiifc$. This string is not a palindrome at first glance. But if we rotate the string R indices counter-clockwise, we get $B = behjgdacfiifcadgjheb$. This is a palindrome.

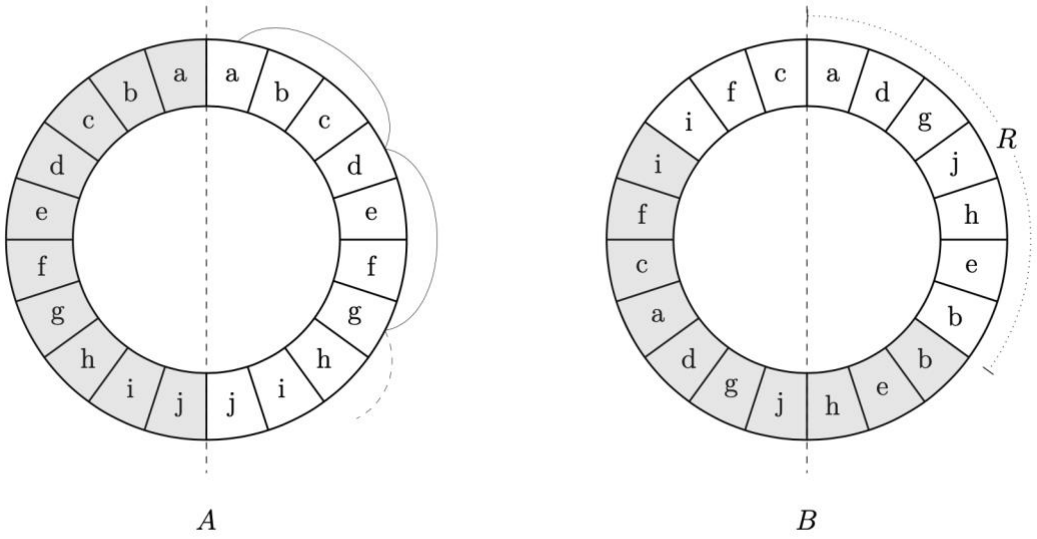


Fig 3.3: Cyclic Shift of A with $s \neq s^*$ resulting in B.

Section 5: References

[1] Wikipedia - Multiplicative group of integers modulo n

[2] Math StackExchange - Proof