Words that almost commute

Daniel Gabric

University of Waterloo

November 22, 2021

Words that commute

- When does $xy = yx$ for non-empty words x, y?

Words that commute

- When does $xy = yx$ for non-empty words x, y?

Theorem (Lyndon-Schützenberger)

Let x and y be non-empty words. Then $xy = yx$ if and only if there exists a non-empty word z, and integers $i, j \geq 1$ such that $x = z^i$ and $y = z^j$.

Words that commute

- When does $xy = yx$ for non-empty words x, y?

Theorem (Lyndon-Schützenberger)

Let x and y be non-empty words. Then $xy = yx$ if and only if there exists a non-empty word z, and integers $i, j \geq 1$ such that $x = z^i$ and $y = z^j$.

- A word w is a *power* if $w = u^i$ for some non-empty word u and some integer $i \geq 2$. Otherwise, w is said to be *primitive*.

Words that commute

- When does $xy = yx$ for non-empty words x, y?

Theorem (Lyndon-Schützenberger)

Let x and y be non-empty words. Then $xy = yx$ if and only if there exists a non-empty word z, and integers $i, j \geq 1$ such that $x = z^i$ and $y = z^j$.

- A word w is a *power* if $w = u^i$ for some non-empty word u and some integer $i \geq 2$. Otherwise, w is said to be *primitive*.
- Two words x and y commute if and only if xy and yx are powers of the same word.

Words that commute

- When does $xy = yx$ for non-empty words x, y?

Theorem (Lyndon-Schützenberger)

Let x and y be non-empty words. Then $xy = yx$ if and only if there exists a non-empty word z, and integers $i, j \geq 1$ such that $x = z^i$ and $y = z^j$.

- A word w is a *power* if $w = u^i$ for some non-empty word u and some integer $i \geq 2$. Otherwise, w is said to be *primitive*.
- Two words x and y commute if and only if xy and yx are powers of the same word.
- Using this characterization, and a formula for the number of length-n powers, one can count the number of pairs of words (x, y) with $|xy| = n$ that commute.

Fine-Wilf

- Fine and Wilf showed that one can achieve the forward implication of Lyndon-Schützenberger with a weaker hypothesis.

Fine-Wilf

- Fine and Wilf showed that one can achieve the forward implication of Lyndon-Schützenberger with a weaker hypothesis.

Theorem (Fine-Wilf)

Let x and y be non-empty words of lengths m and n. If xy and yx agree on the first $m + n - \gcd(m, n)$ terms then $xy = yx$.

Fine-Wilf

- Fine and Wilf showed that one can achieve the forward implication of Lyndon-Schützenberger with a weaker hypothesis.

Theorem (Fine-Wilf)

Let x and y be non-empty words of lengths m and n. If xy and yx agree on the first $m + n - \gcd(m, n)$ terms then $xy = yx$.

- They showed the optimality of this result by constructing words x and y of lengths m and n such that x and y agree on the first $m + n - \gcd(m, n) - 1$ terms but disagree at position $m + n - \gcd(m, n)$.

Fine-Wilf

- Fine and Wilf showed that one can achieve the forward implication of Lyndon-Schützenberger with a weaker hypothesis.

Theorem (Fine-Wilf)

Let x and y be non-empty words of lengths m and n. If xy and yx agree on the first $m + n - \gcd(m, n)$ terms then $xy = yx$.

- They showed the optimality of this result by constructing words x and y of lengths m and n such that x and y agree on the first $m + n - \gcd(m, n) - 1$ terms but disagree at position $m + n - \gcd(m, n)$.
- Such pairs of words optimally "almost" commute.

Theorem

Let x and y be non-empty words of lengths m and n. If xy and yx agree on the first $m + n - \gcd(m, n) - 1$ positions but disagree at position $m + n - \gcd(m, n)$ then xy and yx differ in exactly 2 positions.

Smallest Hamming distance

- The *Hamming distance* $\text{ham}(u, v)$ between two equal-length words u, v is defined to be the number of positions where u and v differ.

Smallest Hamming distance

- The *Hamming distance* $\text{ham}(u, v)$ between two equal-length words u, v is defined to be the number of positions where u and v differ.
- Shallit proved that the smallest value $\text{ham}(xy, yx)$ can take on, other than 0, is 2.

Smallest Hamming distance

- The *Hamming distance* $\text{ham}(u, v)$ between two equal-length words u, v is defined to be the number of positions where u and v differ.
- Shallit proved that the smallest value $\text{ham}(xy, yx)$ can take on, other than 0, is 2.

Theorem (Shallit [1])

Let x and y be words. Then $\text{ham}(xy, yx) \neq 1$.

Smallest Hamming distance

- The *Hamming distance* $\text{ham}(u, v)$ between two equal-length words u, v is defined to be the number of positions where u and v differ.
- Shallit proved that the smallest value $\text{ham}(xy, yx)$ can take on, other than 0, is 2.

Theorem (Shallit [1])

Let x and y be words. Then $\text{ham}(xy, yx) \neq 1$.

Proof.

The proof is by contradiction. Suppose $\text{ham}(xy, yx) = 1$. Then $xy = uav$ and $yx = ubv$ where a, b are distinct symbols. But this means that xy and yx have different counts of a's and b's. A contradiction. □

[1] Jeffrey Shallit. Hamming distance for conjugates. Discrete Mathematics, 309(12):4197–4199, 2009.

Words that almost commute

- If $\mathrm{ham}(xy, yx) = 2$ we say that x and y *almost commute*.

Words that almost commute

- If $\text{ham}(xy, yx) = 2$ we say that x and y *almost commute*.
- The words xy and yx are said to be *conjugates*.

Words that almost commute

- If $\mathrm{ham}(xy, yx) = 2$ we say that x and y *almost commute*.
- The words xy and yx are said to be *conjugates*.
- So we could, equivalently, either talk about pairs of words (x, y) that almost commute, or we could talk about words u that have a conjugate v such that $\mathrm{ham}(u, v) = 2$.

Words that almost commute

- If $\text{ham}(xy, yx) = 2$ we say that x and y *almost commute*.
- The words xy and yx are said to be *conjugates*.
- So we could, equivalently, either talk about pairs of words (x, y) that almost commute, or we could talk about words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Can we characterize almost-commuting pairs of words in a similar way that Lyndon and Schützenberger characterized commuting pairs of words?

Words that almost commute

- If $\text{ham}(xy, yx) = 2$ we say that x and y *almost commute*.
- The words xy and yx are said to be *conjugates*.
- So we could, equivalently, either talk about pairs of words (x, y) that almost commute, or we could talk about words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Can we characterize almost-commuting pairs of words in a similar way that Lyndon and Schützenberger characterized commuting pairs of words?
- Can we count the number of almost-commuting pairs of words?

Words that almost commute

- If $\text{ham}(xy, yx) = 2$ we say that x and y *almost commute*.
- The words xy and yx are said to be *conjugates*.
- So we could, equivalently, either talk about pairs of words (x, y) that almost commute, or we could talk about words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Can we characterize almost-commuting pairs of words in a similar way that Lyndon and Schützenberger characterized commuting pairs of words?
- Can we count the number of almost-commuting pairs of words?
- In this talk, we answer these questions using the conjugate formulation.

Results

- A characterization of length-n words u that have a conjugate v such that $\mathrm{ham}(u, v) = 2$.

Results

- A characterization of length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n words u that have exactly one conjugate v such that $\text{ham}(u, v) = 2$.

Results

- A characterization of length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n words u that have exactly one conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n Lyndon words u that have a conjugate v such that $\text{ham}(u, v) = 2$.

Results

- A characterization of length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n words u that have exactly one conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n Lyndon words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Formulas for all of these quantities.

Results

- A characterization of length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n words u that have exactly one conjugate v such that $\text{ham}(u, v) = 2$.
- A characterization of length-n Lyndon words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Formulas for all of these quantities.
- Asymptotic behaviour.

Notation

- All of the following definitions are assumed to be over a k-letter alphabet $\Sigma_k = \{0, 1, \ldots, k-1\}$.

Notation

- All of the following definitions are assumed to be over a k-letter alphabet $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- Let σ be the left-shift map, so that $\sigma^{|x|}(xy) = yx$ for any words x, y.

Notation

- All of the following definitions are assumed to be over a k-letter alphabet $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- Let σ be the left-shift map, so that $\sigma^{|x|}(xy) = yx$ for any words x, y.
- Let $H(n)$ denote the set of all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.

Notation

- All of the following definitions are assumed to be over a k-letter alphabet $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- Let σ be the left-shift map, so that $\sigma^{|x|}(xy) = yx$ for any words x, y.
- Let $H(n)$ denote the set of all length-n words u that have a conjugate v such that $\mathrm{ham}(u, v) = 2$.
- Let $h(n) = |H(n)|$.

Notation

- All of the following definitions are assumed to be over a k-letter alphabet $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- Let σ be the left-shift map, so that $\sigma^{|x|}(xy) = yx$ for any words x, y.
- Let $H(n)$ denote the set of all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Let $h(n) = |H(n)|$.
- Let $H(n, i)$ denote the set of all length-n words u such that $\text{ham}(u, \sigma^i(u)) = 2$.

Notation

- All of the following definitions are assumed to be over a k-letter alphabet $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- Let σ be the left-shift map, so that $\sigma^{|x|}(xy) = yx$ for any words x, y.
- Let $H(n)$ denote the set of all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$.
- Let $h(n) = |H(n)|$.
- Let $H(n, i)$ denote the set of all length-n words u such that $\text{ham}(u, \sigma^i(u)) = 2$.
- Let $h(n, i) = |H(n, i)|$.

Useful property

Lemma

Let u be a length-n word. Let i be an integer with $0 < i < n$. If $u \in H(n, i)$ then $u \in H(n, n - i)$.

Proof.

Useful property

Lemma

Let u be a length-n word. Let i be an integer with $0 < i < n$. If $u \in H(n, i)$ then $u \in H(n, n - i)$.

Proof.

Suppose $i \leq n/2$. Then we can write $u = xtz$ for some words t, z where $|x| = |z| = i$ and $|t| = n - 2i$. We have that $\text{ham}(xtz, tzx) = \text{ham}(xt, tz) + \text{ham}(z, x) = 2$. Consider the word zxt. Clearly $v = zxt$ is a conjugate of $u = xtz$ such that $\text{ham}(xtz, zxt) = \text{ham}(x, z) + \text{ham}(tz, xt) = 2$ where $u = (xt)z$ and $v = z(xt)$ with $|xt| = n - i$. Therefore $u \in H(n, n - i)$.

Useful property

Lemma

Let u be a length-n word. Let i be an integer with $0 < i < n$. If $u \in H(n, i)$ then $u \in H(n, n-i)$.

Proof.

Suppose $i \leq n/2$. Then we can write $u = xtz$ for some words t, z where $|x| = |z| = i$ and $|t| = n - 2i$. We have that $\text{ham}(xtz, tzx) = \text{ham}(xt, tz) + \text{ham}(z, x) = 2$. Consider the word zxt. Clearly $v = zxt$ is a conjugate of $u = xtz$ such that $\text{ham}(xtz, zxt) = \text{ham}(x, z) + \text{ham}(tz, xt) = 2$ where $u = (xt)z$ and $v = z(xt)$ with $|xt| = n - i$. Therefore $u \in H(n, n-i)$.

Suppose $i > n/2$. Then we can write $u = zty$ for some words t, z where $|z| = |y| = n - i$ and $|t| = 2i - n$. We have that $\text{ham}(zty, yzt) = \text{ham}(z, y) + \text{ham}(ty, zt) = 2$. Consider the word tyz. Clearly $v = tyz$ is a conjugate of $u = zty$ such that $\text{ham}(zty, tyz) = \text{ham}(zt, ty) + \text{ham}(y, z) = 2$ where $u = z(ty)$ and $v = (ty)z$ with $|z| = n - i$. Therefore $u \in H(n, n-i)$. □

Characterizing $H(n,i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n,i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \le j \le n/g - 1$. Then $w \in H(n,i)$ iff there exist two distinct integers j_1, j_2, $0 \le j_1 < j_2 \le n/g - 1$ such that $\mathrm{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \ne j_1, j_2$, $0 \le j \le n/g - 1$.

- Suppose $w \in H(n,i)$.

Characterizing $H(n, i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n, i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \le j \le n/g - 1$. Then $w \in H(n, i)$ iff there exist two distinct integers j_1, j_2, $0 \le j_1 < j_2 \le n/g - 1$ such that $\text{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \ne j_1, j_2$, $0 \le j \le n/g - 1$.

- Suppose $w \in H(n, i)$.
- Write $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all meaningful j.

Characterizing $H(n,i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n,i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \le j \le n/g - 1$. Then $w \in H(n,i)$ iff there exist two distinct integers j_1, j_2, $0 \le j_1 < j_2 \le n/g - 1$ such that $\text{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \ne j_1, j_2$, $0 \le j \le n/g - 1$.

- Suppose $w \in H(n,i)$.
- Write $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all meaningful j.

$$\begin{aligned}\text{ham}(w, \sigma^i(w)) &= \text{ham}(x_0 x_1 \cdots x_{n/g-1}, x_{i/g} \cdots x_{n/g-1} x_0 \cdots x_{i/g-1}) \\ &= \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2\end{aligned}$$

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:
  1. There exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:
  1. There exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
  2. There exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:
  1. There exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
  2. There exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Suppose there exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:
  1. There exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
  2. There exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Suppose there exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
- Then $\text{ham}(x_{j'}, x_{(j'+i/g) \bmod n/g}) = 0$ for all meaningful $j' \neq j$.

Characterizing $H(n, i)$

$$\text{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:
  1. There exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
  2. There exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Suppose there exists a single j such that $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
- Then $\text{ham}(x_{j'}, x_{(j'+i/g) \bmod n/g}) = 0$ for all meaningful $j' \neq j$.
- The additive order of i/g modulo n/g is $\frac{n/g}{\gcd(n/g, i/g)} = n/g$.

Characterizing $H(n, i)$

$$\mathrm{ham}(w, \sigma^i(w)) = \sum_{j=0}^{n/g-1} \mathrm{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$$

- One of the following must be true:
  1. There exists a single j such that $\mathrm{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
  2. There exist two distinct integers j_1, j_2 such that $\mathrm{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \mathrm{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Suppose there exists a single j such that $\mathrm{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$.
- Then $\mathrm{ham}(x_{j'}, x_{(j'+i/g) \bmod n/g}) = 0$ for all meaningful $j' \neq j$.
- The additive order of i/g modulo n/g is $\frac{n/g}{\gcd(n/g, i/g)} = n/g$.
- Thus

$$x_{(j+i/g) \bmod n/g} = x_{(j+2i/g) \bmod n/g} = \cdots = x_{(j+(n/g-1)i/g) \bmod n/g} = x_j$$

and $\mathrm{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 2$, a contradiction.

Characterizing $H(n, i)$

- Suppose there exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.

Characterizing $H(n, i)$

- Suppose there exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Then $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 0$ for all meaningful $j \neq j_1, j_2$.

Characterizing $H(n, i)$

- Suppose there exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Then $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 0$ for all meaningful $j \neq j_1, j_2$.
- So

$$x_{(j_1+i/g) \bmod n/g} = x_{(j_1+2i/g) \bmod n/g} = \cdots = x_{j_2}$$

and

$$x_{(j_2+i/g) \bmod n/g} = x_{(j_2+2i/g) \bmod n/g} = \cdots = x_{j_1}$$

Characterizing $H(n, i)$

- Suppose there exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Then $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 0$ for all meaningful $j \neq j_1, j_2$.
- So

$$x_{(j_1+i/g) \bmod n/g} = x_{(j_1+2i/g) \bmod n/g} = \cdots = x_{j_2}$$

and

$$x_{(j_2+i/g) \bmod n/g} = x_{(j_2+2i/g) \bmod n/g} = \cdots = x_{j_1}$$

- Thus $\text{ham}(x_{j_1}, x_{j_2}) = 1$.

Characterizing $H(n, i)$

- Suppose there exist two distinct integers j_1, j_2 such that $\text{ham}(x_{j_1}, x_{(j_1+i/g) \bmod n/g}) = \text{ham}(x_{j_2}, x_{(j_2+i/g) \bmod n/g}) = 1$.
- Then $\text{ham}(x_j, x_{(j+i/g) \bmod n/g}) = 0$ for all meaningful $j \neq j_1, j_2$.
- So

$$x_{(j_1+i/g) \bmod n/g} = x_{(j_1+2i/g) \bmod n/g} = \cdots = x_{j_2}$$

  and

$$x_{(j_2+i/g) \bmod n/g} = x_{(j_2+2i/g) \bmod n/g} = \cdots = x_{j_1}$$

- Thus $\text{ham}(x_{j_1}, x_{j_2}) = 1$.
- Other direction is easy.

Counting $H(n, i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n, i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \le j \le n/g - 1$. Then $w \in H(n, i)$ iff there exist two distinct integers j_1, j_2, $0 \le j_1 < j_2 \le n/g - 1$ such that $\mathrm{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \ne j_1, j_2$, $0 \le j \le n/g - 1$.

Counting $H(n, i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n, i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \leq j \leq n/g - 1$. Then $w \in H(n, i)$ iff there exist two distinct integers j_1, j_2, $0 \leq j_1 < j_2 \leq n/g - 1$ such that $\text{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \neq j_1, j_2$, $0 \leq j \leq n/g - 1$.

- There are $\sum_{j_2=1}^{n/g-1} \sum_{j_1=0}^{j_2-1} 1 = \frac{1}{2} \frac{n}{g} \left(\frac{n}{g} - 1 \right)$ choices for j_1 and j_2.

Counting $H(n, i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n, i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \le j \le n/g - 1$. Then $w \in H(n, i)$ iff there exist two distinct integers j_1, j_2, $0 \le j_1 < j_2 \le n/g - 1$ such that $\text{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \ne j_1, j_2$, $0 \le j \le n/g - 1$.

- There are $\sum_{j_2=1}^{n/g-1} \sum_{j_1=0}^{j_2-1} 1 = \frac{1}{2}\frac{n}{g}\left(\frac{n}{g} - 1\right)$ choices for j_1 and j_2.
- There are k^g choices for x_{j_1}.

Counting $H(n, i)$

Lemma

Let n, i be positive integers such that $n > i$. Let $g = \gcd(n, i)$. Let w be a length-n word. Let $w = x_0 x_1 \cdots x_{n/g-1}$ where $|x_j| = g$ for all j, $0 \le j \le n/g - 1$. Then $w \in H(n, i)$ iff there exist two distinct integers j_1, j_2, $0 \le j_1 < j_2 \le n/g - 1$ such that $\operatorname{ham}(x_{j_1}, x_{j_2}) = 1$ and $x_j = x_{(j+i/g) \bmod n/g}$ for all $j \ne j_1, j_2$, $0 \le j \le n/g - 1$.

- There are $\sum_{j_2=1}^{n/g-1} \sum_{j_1=0}^{j_2-1} 1 = \frac{1}{2}\frac{n}{g}\left(\frac{n}{g} - 1\right)$ choices for j_1 and j_2.
- There are k^g choices for x_{j_1}.
- There are $n(k-1)$ choices for x_{j_2} given x_{j_1}.

Theorem

Let n, i be positive integers such that $n > i$. Then

$$h(n, i) = \frac{1}{2} k^{\gcd(n,i)} (k-1) n \left(\frac{n}{\gcd(n, i)} - 1 \right).$$

Counting $H(n)$

- Since $H(n, i) = H(n, n - i)$, we only need to concern ourselves with $H(n, i)$ for $i \leq n/2$.

Counting $H(n)$

- Since $H(n,i) = H(n,n-i)$, we only need to concern ourselves with $H(n,i)$ for $i \leq n/2$.
- Clearly $h(n) \leq \sum_{i=1}^{\lfloor n/2 \rfloor} h(n,i)$.

Counting $H(n)$

- Since $H(n,i) = H(n,n-i)$, we only need to concern ourselves with $H(n,i)$ for $i \leq n/2$.
- Clearly $h(n) \leq \sum_{i=1}^{\lfloor n/2 \rfloor} h(n,i)$.
- But in the sum we are double counting those words w that are in multiple $H(n,i)$.

Counting $H(n)$

- Since $H(n, i) = H(n, n - i)$, we only need to concern ourselves with $H(n, i)$ for $i \leq n/2$.
- Clearly $h(n) \leq \sum_{i=1}^{\lfloor n/2 \rfloor} h(n, i)$.
- But in the sum we are double counting those words w that are in multiple $H(n, i)$.
- Similar to the Fine-Wilf theorem, we need a characterization of words that are in $H(n, i)$ and $H(n, j)$ for $i \neq j$.

Counting $H(n)$

- Since $H(n,i) = H(n,n-i)$, we only need to concern ourselves with $H(n,i)$ for $i \le n/2$.
- Clearly $h(n) \le \sum_{i=1}^{\lfloor n/2 \rfloor} h(n,i)$.
- But in the sum we are double counting those words w that are in multiple $H(n,i)$.
- Similar to the Fine-Wilf theorem, we need a characterization of words that are in $H(n,i)$ and $H(n,j)$ for $i \ne j$.

Lemma

Let n, i, j be positive integers such that $n \ge 2i > 2j$. Let $g = \gcd(n,i,j)$. Let w be a length-n word. Then $w \in H(n,i)$ and $w \in H(n,j)$ if and only if there exists a word u of length g, a word v of length g with $\mathrm{ham}(u,v) = 1$, and a non-negative integer $p < n/g$ such that $w = u^p v u^{n/g-p-1}$.

Counting $H(n)$

- Since $H(n, i) = H(n, n - i)$, we only need to concern ourselves with $H(n, i)$ for $i \leq n/2$.
- Clearly $h(n) \leq \sum_{i=1}^{\lfloor n/2 \rfloor} h(n, i)$.
- But in the sum we are double counting those words w that are in multiple $H(n, i)$.
- Similar to the Fine-Wilf theorem, we need a characterization of words that are in $H(n, i)$ and $H(n, j)$ for $i \neq j$.

Lemma

Let n, i, j be positive integers such that $n \geq 2i > 2j$. Let $g = \gcd(n, i, j)$. Let w be a length-n word. Then $w \in H(n, i)$ and $w \in H(n, j)$ if and only if there exists a word u of length g, a word v of length g with $\text{ham}(u, v) = 1$, and a non-negative integer $p < n/g$ such that $w = u^p v u^{n/g-p-1}$.

- A word w is in multiple $H(n, i)$ if it is Hamming distance 1 away from a power (of exponent 4 or greater).

Counting $H(n)$

- Let $p_k(n)$ denote the number of length-n powers.

Counting $H(n)$

- Let $p_k(n)$ denote the number of length-n powers.

Theorem

Let n be a positive integer. Then

$$h(n) = \sum_{i=1}^{\lfloor n/2 \rfloor} h(n,i) - h'(n,i)$$

where

$$h'(n,i) = \begin{cases} n(k-1)p_k(i), & \text{if } i \mid n; \\ n(k-1)k^{\gcd(n,i)}, & \text{otherwise.} \end{cases}$$

Counting words with exactly one conjugate

- What about the number of length-n words u that have exactly one conjugate v with $\text{ham}(u, v) = 2$?

Counting words with exactly one conjugate

- What about the number of length-n words u that have exactly one conjugate v with $\text{ham}(u, v) = 2$?
- Let w be such a length-n word.

Counting words with exactly one conjugate

- What about the number of length-n words u that have exactly one conjugate v with $\text{ham}(u, v) = 2$?
- Let w be such a length-n word.
- Since $H(n, i) = H(n, n - i)$, we must have that n is even and $w \in H(n, n/2)$.

Counting words with exactly one conjugate

- What about the number of length-n words u that have exactly one conjugate v with $\text{ham}(u, v) = 2$?
- Let w be such a length-n word.
- Since $H(n, i) = H(n, n - i)$, we must have that n is even and $w \in H(n, n/2)$.
- But w cannot be in any $H(n, j)$ for $j < n/2$.

Counting words with exactly one conjugate

- What about the number of length-n words u that have exactly one conjugate v with $\text{ham}(u, v) = 2$?
- Let w be such a length-n word.
- Since $H(n, i) = H(n, n - i)$, we must have that n is even and $w \in H(n, n/2)$.
- But w cannot be in any $H(n, j)$ for $j < n/2$.

Theorem

Let n be a positive integer. If n is odd, then there are 0 length-n words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$. If n is even, then there are

$$h(n, n/2) - n(k - 1)p_k(n/2)$$

length-n words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$.

Lyndon conjugates

- A word w is said to be a *Lyndon word* if it is strictly smaller than all of its non-trivial conjugates.

Lyndon conjugates

- A word w is said to be a *Lyndon word* if it is strictly smaller than all of its non-trivial conjugates.
  - All Lyndon words are primitive.

Lyndon conjugates

- A word w is said to be a *Lyndon word* if it is strictly smaller than all of its non-trivial conjugates.
  - All Lyndon words are primitive.

Theorem

There are $\frac{h(n)}{n}$ length-n Lyndon words u that have a conjugate v such that $\mathrm{ham}(u, v) = 2$.

Lyndon conjugates

- A word w is said to be a *Lyndon word* if it is strictly smaller than all of its non-trivial conjugates.
  - All Lyndon words are primitive.

Theorem

There are $\frac{h(n)}{n}$ length-n Lyndon words u that have a conjugate v such that $\text{ham}(u, v) = 2$.

- Clearly $\text{ham}(w, \sigma^i(w)) = \text{ham}(\sigma^j(w), \sigma^{i+j}(w))$. So if $w \in H(n)$, then any conjugate of w is also in $H(n)$.

Lyndon conjugates

- A word w is said to be a *Lyndon word* if it is strictly smaller than all of its non-trivial conjugates.
  - All Lyndon words are primitive.

Theorem

There are $\frac{h(n)}{n}$ length-n Lyndon words u that have a conjugate v such that $\text{ham}(u, v) = 2$.

- Clearly $\text{ham}(w, \sigma^i(w)) = \text{ham}(\sigma^j(w), \sigma^{i+j}(w))$. So if $w \in H(n)$, then any conjugate of w is also in $H(n)$.
- All that is left is to prove that every element of $H(n)$ is primitive.

Lyndon conjugates

- Suppose that $w \in H(n)$ is a power. Then $w = u^m$ for some non-empty word u, and some $m \geq 2$.

Lyndon conjugates

- Suppose that $w \in H(n)$ is a power. Then $w = u^m$ for some non-empty word u, and some $m \geq 2$.
- Any conjugate of w is of the form $(ts)^m$ where $u = st$.

Lyndon conjugates

- Suppose that $w \in H(n)$ is a power. Then $w = u^m$ for some non-empty word u, and some $m \geq 2$.
- Any conjugate of w is of the form $(ts)^m$ where $u = st$.
- Let $w' = (ts)^m$ be a conjugate of $w = (st)^m$ such that $\text{ham}(w, w') = 2$.

Lyndon conjugates

- Suppose that $w \in H(n)$ is a power. Then $w = u^m$ for some non-empty word u, and some $m \geq 2$.
- Any conjugate of w is of the form $(ts)^m$ where $u = st$.
- Let $w' = (ts)^m$ be a conjugate of $w = (st)^m$ such that $\text{ham}(w, w') = 2$.
- We have $\text{ham}(w, w') = \text{ham}((st)^m, (ts)^m) = m\,\text{ham}(st, ts)$.

Lyndon conjugates

- Suppose that $w \in H(n)$ is a power. Then $w = u^m$ for some non-empty word u, and some $m \geq 2$.
- Any conjugate of w is of the form $(ts)^m$ where $u = st$.
- Let $w' = (ts)^m$ be a conjugate of $w = (st)^m$ such that $\text{ham}(w, w') = 2$.
- We have $\text{ham}(w, w') = \text{ham}((st)^m, (ts)^m) = m\,\text{ham}(st, ts)$.
- We have that $\text{ham}(st, ts) = 0$ or $\text{ham}(st, ts) \geq 2$.

Lyndon conjugates

- Suppose that $w \in H(n)$ is a power. Then $w = u^m$ for some non-empty word u, and some $m \geq 2$.
- Any conjugate of w is of the form $(ts)^m$ where $u = st$.
- Let $w' = (ts)^m$ be a conjugate of $w = (st)^m$ such that $\text{ham}(w, w') = 2$.
- We have $\text{ham}(w, w') = \text{ham}((st)^m, (ts)^m) = m\,\text{ham}(st, ts)$.
- We have that $\text{ham}(st, ts) = 0$ or $\text{ham}(st, ts) \geq 2$.
- In either case, $\text{ham}(w, w') \neq 2$, a contradiction.

Asymptotic behaviour of $h(n)$

Lemma

Let n be a prime number. Then $h(n) = \frac{1}{4}k(k-1)n(n^2 - 4n + 7)$.

Asymptotic behaviour of $h(n)$

Lemma

Let n be a prime number. Then $h(n) = \frac{1}{4}k(k-1)n(n^2 - 4n + 7)$.

- Since $\gcd(n, i) = 1$ for all i, $1 < i \leq n/2$, it is easy to simplify the sum for $h(n)$ to get the resulting polynomial.

Asymptotic behaviour of $h(n)$

Lemma

Let n be a prime number. Then $h(n) = \frac{1}{4}k(k-1)n(n^2 - 4n + 7)$.

- Since $\gcd(n, i) = 1$ for all i, $1 < i \leq n/2$, it is easy to simplify the sum for $h(n)$ to get the resulting polynomial.

Lemma

Let $n > 1$ be an integer. Then $h(2n) \geq \frac{1}{2}nk^n$.

Asymptotic behaviour of $h(n)$

Lemma

Let n be a prime number. Then $h(n) = \frac{1}{4}k(k-1)n(n^2-4n+7)$.

- Since $\gcd(n, i) = 1$ for all i, $1 < i \leq n/2$, it is easy to simplify the sum for $h(n)$ to get the resulting polynomial.

Lemma

Let $n > 1$ be an integer. Then $h(2n) \geq \frac{1}{2}nk^n$.

Proof.

$H(2n, n)$ is a subset of $H(2n)$. Therefore
$h(2n) \geq h(2n, n) \geq \frac{1}{2}(k-1)nk^n \geq \frac{1}{2}nk^n$. □

Asymptotic behaviour of $h(n)$

Lemma

Let n be a prime number. Then $h(n) = \frac{1}{4}k(k-1)n(n^2-4n+7)$.

- Since $\gcd(n,i) = 1$ for all i, $1 < i \leq n/2$, it is easy to simplify the sum for $h(n)$ to get the resulting polynomial.

Lemma

Let $n > 1$ be an integer. Then $h(2n) \geq \frac{1}{2}nk^n$.

Proof.

$H(2n, n)$ is a subset of $H(2n)$. Therefore
$h(2n) \geq h(2n, n) \geq \frac{1}{2}(k-1)nk^n \geq \frac{1}{2}nk^n$. □

- So $h(n)$ behaves as a polynomial for infinitely many n, and as an exponential for infinitely many n.

Asymptotic behaviour of $h(n)$

Lemma

Let n be a prime number. Then $h(n) = \frac{1}{4}k(k-1)n(n^2 - 4n + 7)$.

- Since $\gcd(n, i) = 1$ for all i, $1 < i \leq n/2$, it is easy to simplify the sum for $h(n)$ to get the resulting polynomial.

Lemma

Let $n > 1$ be an integer. Then $h(2n) \geq \frac{1}{2}nk^n$.

Proof.

$H(2n, n)$ is a subset of $H(2n)$. Therefore
$h(2n) \geq h(2n, n) \geq \frac{1}{2}(k-1)nk^n \geq \frac{1}{2}nk^n$. □

- So $h(n)$ behaves as a polynomial for infinitely many n, and as an exponential for infinitely many n.
- No one easily-expressible bound on $h(n)$.

Conclusions

- We characterized and counted all length-n words u that have a conjugate v such that $\mathrm{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179674`.

Conclusions

- We characterized and counted all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179674`.
  - One can use this formula to count the number of pairs of almost-commuting words (x, y) with $|xy| = n$.

Conclusions

- We characterized and counted all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179674`.
  - One can use this formula to count the number of pairs of almost-commuting words (x, y) with $|xy| = n$.
- We characterized and counted all length-n words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179677`.

Conclusions

- We characterized and counted all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179674`.
  - One can use this formula to count the number of pairs of almost-commuting words (x, y) with $|xy| = n$.
- We characterized and counted all length-n words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179677`.
- We also characterized and counted all length-n Lyndon words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A226893`.

Conclusions

- We characterized and counted all length-n words u that have a conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179674`.
  - One can use this formula to count the number of pairs of almost-commuting words (x, y) with $|xy| = n$.
- We characterized and counted all length-n words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A179677`.
- We also characterized and counted all length-n Lyndon words u with exactly one conjugate v such that $\text{ham}(u, v) = 2$. Formula corresponds to the sequence: `https://oeis.org/A226893`.
- Finally, we showed that there is no one easily-expressible bound for $h(n)$ by showing that $h(n)$ behaves as a polynomial for all prime n, and that $h(n)$ behaves as an exponential for all even n.