FFT - התמרת פורייה המהירה

מפגש 8

בוא נזכר מה התחלנו שבוע שעבר

בוא נזכר מה התחלנו שבוע שעבר

- נזכרנו שקונבולוציה אנחנו מכירים כבר ממזמן - זה בעצם הפעולה שאנחנו עושים שאנחנו מכפילים שני פולינומים

בוא נזכר מה התחלנו שבוע שעבר

- נזכרנו שקונבולוציה אנחנו מכירים כבר ממזמן - זה בעצם הפעולה שאנחנו עושים שאנחנו מכפילים שני פולינומים
- למעשה - לחשב את הקונבולוציה של שני וקטורים שקול ללחשב הכפלה של שני פולינומים

קונבולוציה - הגדרה

קונבולוציה - הגדרה

- בהינתן שני וקטורים

$$A = (a_0, a_1, \ldots, a_n)$$

$$B = (b_0, b_1, \ldots, b_m)$$

קונבולוציה - הגדרה

- בהינתן שני וקטורים

$$A = (a_0, a_1, \ldots, a_n)$$

$$B = (b_0, b_1, \ldots, b_m)$$

- קונבולוציה של A עם B מסומנת ב: $A * B = C$

קונבולוציה - הגדרה

- בהינתן שני וקטורים

$$A = (a_0, a_1, \ldots, a_n)$$

$$B = (b_0, b_1, \ldots, b_m)$$

- קונבולוציה של A עם B מסומנת ב: $A * B = C$
- עבור וקטור C באורך $m + n + 1$ המוגדר כך:

$$c_i = \sum_{j,k:j+k=i} a_j \cdot b_k$$

ייצוג פולינומים

בהינתן פולינום מדרגה m ניתן לייצג אותו:

ייצוג פולינומים

בהינתן פולינום מדרגה n ניתן לייצג אותו:

- ע"י $n+1$ מקדמים

ייצוג פולינומים

בהינתן פולינום מדרגה n ניתן לייצג אותו:

- ע"י $n+1$ מקדמים
- ע"י $n+1$ נקודות

ייצוג פולינומים

בהינתן פולינום מדרגה n ניתן לייצג אותו:

- ע"י $n+1$ מקדמים
- ע"י $n+1$ נקודות

ייצוג פולינומים

בהינתן פולינום מדרגה n ניתן לייצג אותו:

- ע"י $n+1$ מקדמים
- ע"י $n+1$ נקודות

המשפט היסודי של האלגברה: דרך $n+1$ נקודות עובר פולינום יחיד ממעלה n

ההבדלים בין הייצוגים

ההבדלים בין הייצוגים

- קבלת הערך בנקודה

ההבדלים בין הייצוגים

- קבלת הערך בנקודה
- מכפלת שני פולינומים

ההבדלים בין הייצוגים

- קבלת הערך בנקודה
- מכפלת שני פולינומים

ההבדלים בין הייצוגים

- קבלת הערך בנקודה
- מכפלת שני פולינומים
  - בייצוג מקדמים - דורש זמן ריבועי

ההבדלים בין הייצוגים

- קבלת הערך בנקודה
- מכפלת שני פולינומים
  - בייצוג מקדמים - דורש זמן ריבועי
  - בייצוג בנקודות - אם יש לנו $2n+1$ נקודות של כל פולינום ניתן לחשב בזמן לינארי

סקיצה לאלגוריתם לחישוב קונבולוציה

על מנת לחשב את $C = A * B$

סקיצה לאלגוריתם לחישוב קונבולוציה

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות

סקיצה לאלגוריתם לחישוב קונבולוציה

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות
2. נכפול נקודתית את ערכי A ו-B

סקיצה לאלגוריתם לחישוב קונבולוציה

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות
2. נכפול נקודתית את ערכי A ו-B
3. נחשב את מקדמי הפולינום C מתוך הנקודות

סקיצה לאלגוריתם לחישוב קונבולוציה

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות
2. נכפול נקודתית את ערכי A ו-B
3. נחשב את מקדמי הפולינום C מתוך הנקודות

סקיצה לאלגוריתם לחישוב קונבולוציה

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות
2. נכפול נקודתית את ערכי A ו-B
3. נחשב את מקדמי הפולינום C מתוך הנקודות

כיצד נעבור מייצוג לייצוג בצורה יעילה? (מהירה יותר מ-$\Theta(n^2)$).

דוגמא לחישוב פולינום ב-n נקודות

אז מצאנו שיטה הפרד ומשול לחישוב פולינום בנקודות

אז מצאנו שיטה הפרד ומשול לחישוב פולינום בנקודות

- בהינתן פולינום המיוצג על ידי מקדמים: $p = (a_0, a_1, \ldots, a_{n-1})$

אז מצאנו שיטה הפרד ומשול לחישוב פולינום בנקודות

- בהינתן פולינום המיוצג על ידי מקדמים: $p = (a_0, a_1, \ldots, a_{n-1})$
- בנה שני פולינומים:

$$p_{odd} = (a_1, a_3, \ldots, a_{n-1})$$

$$p_{even} = (a_0, a_2, \ldots, a_{n-2})$$

אז מצאנו שיטה הפרד ומשול לחישוב פולינום בנקודות

- בהינתן פולינום המיוצג על ידי מקדמים: $p = (a_0, a_1, \ldots, a_{n-1})$
- בנה שני פולינומים:

$$p_{odd} = (a_1, a_3, \ldots, a_{n-1})$$

$$p_{even} = (a_0, a_2, \ldots, a_{n-2})$$

- חשב רקורסיבית $\frac{n}{2}$ ערכים של p_{odd} ו- p_{even} בנקודות:

$$t_1^2, t_2^2, t_{\frac{n}{2}}^2$$

אז מצאנו שיטה הפרד ומשול לחישוב פולינום בנקודות

- בהינתן פולינום המיוצג על ידי מקדמים: $p = (a_0, a_1, \ldots, a_{n-1})$
- בנה שני פולינומים:

$$p_{odd} = (a_1, a_3, \ldots, a_{n-1})$$

$$p_{even} = (a_0, a_2, \ldots, a_{n-2})$$

- חשב רקורסיבית $\frac{n}{2}$ ערכים של p_{odd} ו- p_{even} בנקודות:

$$t_1^2, t_2^2, t_{\frac{n}{2}}^2$$

- לכל $z \in \{t_i, -t_i : 1 \leq i \leq \frac{n}{2}\}$ מצא את ערכי $p(z)$ ע"י הנוסחא:

$$p(x) = p_{even}(x^2) + xp_{odd}(x^2)$$

סה"כ n נקודות.

תרגיל

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(-2, 2, -1, 1)$

תרגיל

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(-2, -1, 2, -1, 1)$

- תחילה חשבו את p_{even} ו- p_{odd}.

תרגיל

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(-2, -1, 2, -1, 1)$

- תחילה חשבו את p_{even} ו- p_{odd}.
- לאחר מכן חשבו את הפולינום המוקטנים בנקודות המרובעות ע"י הצבה

תרגיל

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(-2, 2, -1, 1)$

- תחילה חשבו את p_{even} ו- p_{odd}.
- לאחר מכן חשבו את הפולינום המוקטנים בנקודות המרובעות ע"י הצבה
- מצאו את 4 הנקודות הנדרשות ע"י הנוסחא:

$$p(x) = p_{even}(x^2) + xp_{odd}(x^2)$$

חשיבות לבחירת הנקודות

חשיבות לבחירת הנקודות

- אם היינו רוצים רק לחשב פולינום ב-n נקודות כל נקודה $t_i \neq 0$ הייתה עובדת לנו

חשיבות לבחירת הנקודות

- אם היינו רוצים רק לחשב פולינום ב-n נקודות כל נקודה $t_i \neq 0$ הייתה עובדת לנו
- אנחנו רוצים גם לאחר מכן לשחזר את מקדמי פולינום התוצאה (C) מתוך הנקודות

חשיבות לבחירת הנקודות

- אם היינו רוצים רק לחשב פולינום ב-n נקודות כל נקודה $t_i \neq 0$ הייתה עובדת לנו
- אנחנו רוצים גם לאחר מכן לשחזר את מקדמי פולינום התוצאה (C) מתוך הנקודות
- לשם כך אנחנו צריכים לבחור נקודות חכמות שקל יהיה לשחזר מתוכן את הפולינום

חזרה מהירה על מורכבים

חזרה מהירה על מורכבים

- $i^2 = -1$

חזרה מהירה על מורכבים

- $i^2 = -1$
- לפולינום מדרגה n יש n שורשים מעל המורכבים

חזרה מהירה על מורכבים

- $i^2 = -1$
- לפולינום מדרגה n יש n שורשים מעל המורכבים
- לכן למשוואה הזו

$$x^n - 1$$

ישנם בדיוק n שורשים, הנקראים שורשי היחידה

חזרה מהירה על מורכבים

- $i^2 = -1$
- לפולינום מדרגה n יש n שורשים מעל המורכבים
- לכן למשוואה הזו

$$x^n - 1$$

ישנם בדיוק n שורשים, הנקראים שורשי היחידה
- אלו בדיוק n הנקודות שנבחר

שורשי היחידה

$x^n - 1$

שורשי היחידה

$x^n - 1$

- כאשר $n = 2$ מה אלו שורשי היחידה?

שורשי היחידה

$x^n - 1$

- כאשר $n = 2$ מה אלו שורשי היחידה?
- כאשר $n = 4$ שורשי היחידה הם:

$$1, i, -1, -i$$

שורשי היחידה

$x^n - 1$

- כאשר $n = 2$ מה אלו שורשי היחידה?
- כאשר $n = 4$ שורשי היחידה הם:

$$1, i, -1, -i$$

- שורש יחידה כללי מסדר n מסומן ב-$\omega_{j,n}$ ומוגדר כך:

$$\omega_{j,n} = e^{\frac{2\pi i \cdot j}{n}}, \quad j = 0, 1, \ldots, n-1$$

שורשי היחידה

שורשי היחידה

- בואו נוודא שאכן $\omega_{j,n}$ זהו שורש של $x^n - 1$:

$$\omega_{j,n}^n = (e^{\frac{2\pi i \cdot j}{n}})^n = e^{\frac{2\pi i \cdot j \cdot n}{n}} = e^{2\pi i \cdot j} = (e^{2\pi i})^j = 1^j = 1$$

שורשי היחידה

- בואו נוודא שאכן $\omega_{j,n}$ זהו שורש של $x^n - 1$:

$$\omega_{j,n}^n = (e^{\frac{2\pi i \cdot j}{n}})^n = e^{\frac{2\pi i \cdot j \cdot n}{n}} = e^{2\pi i \cdot j} = (e^{2\pi i})^j = 1^j = 1$$

שורשי היחידה

- בואו נוודא שאכן $\omega_{j,n}$ זהו שורש של $x^n - 1$:

$$\omega_{j,n}^{n} = (e^{\frac{2\pi i \cdot j}{n}})^n = e^{\frac{2\pi i \cdot j \cdot n}{n}} = e^{2\pi i \cdot j} = (e^{2\pi i})^j = 1^j = 1$$

* במעבר הלפני האחרון השתמשתנו בזהות אוילר: $e^{2\pi i} = 1$

שורש יחידה פרימיטיבי

שורש יחידה פרימיטיבי

- שורש יחידה פרימיטיבי הוא כזה שלא הופך לאחד באף חזקה פרט ל-n.

שורש יחידה פרימיטיבי

- שורש יחידה פרימיטיבי הוא כזה שלא הופך לאחד באף חזקה פרט ל-n.
- פורמלית: $\omega_{j,n}$ הוא שורש יחידה פרימיטיבי אם

$$\omega_{j,n}^k \neq 1, \quad \forall 0 < k < n$$

שורש יחידה פרימיטיבי

- שורש יחידה פרימיטיבי הוא כזה שלא הופך לאחד באף חזקה פרט ל-n.
- פורמלית: $\omega_{j,n}$ הוא שורש יחידה פרימיטיבי אם

$$\omega_{j,n}^k \neq 1, \quad \forall 0 < k < n$$

- כאשר ידוע מיהו n מסמנים אותו פשוט כך: ω

שורש יחידה פרימיטיבי

- שורש יחידה פרימיטיבי הוא כזה שלא הופך לאחד באף חזקה פרט ל-n.
- פורמלית: $\omega_{j,n}$ הוא שורש יחידה פרימיטיבי אם

$$\omega_{j,n}^k \neq 1, \quad \forall 0 < k < n$$

- כאשר ידוע מיהו n מסמנים אותו פשוט כך: ω
- נבחין שלכל $0 < k < n$:

$$\omega^k = (e^{\frac{2\pi i \cdot j}{n}})^k = e^{\frac{2\pi i \cdot j \cdot k}{n}} \neq 1$$

ולכן ω^k הוא גם שורש יחידה מסדר n (לא פרימיטיבי).

אותו תרגיל בשינוי קטן

חשבו את הפולינום המתאים לקורדינטות הבאות

$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$

אותו תרגיל בשינוי קטן

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$

- תחילה חשבו את p_{even} ו- p_{odd}.

אותו תרגיל בשינוי קטן

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$

- תחילה חשבו את p_{even} ו- p_{odd}.
- לאחר מכן חשבו את הפולינום המוקטנים בנקודות המרובעות ע"י הצבה

אותו תרגיל בשינוי קטן

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$

- תחילה חשבו את p_{even} ו- p_{odd}.
- לאחר מכן חשבו את הפולינום המוקטנים בנקודות המרובעות ע"י הצבה
- מצאו את 4 הנקודות הנדרשות ע"י הנוסחא:

$$p(x) = p_{even}(x^2) + xp_{odd}(x^2)$$

אותו תרגיל בשינוי קטן

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$

- תחילה חשבו את p_{even} ו- p_{odd}.
- לאחר מכן חשבו את הפולינום המוקטנים בנקודות המרובעות ע"י הצבה
- מצאו את 4 הנקודות הנדרשות ע"י הנוסחא:

$$p(x) = p_{even}(x^2) + xp_{odd}(x^2)$$

אותו תרגיל בשינוי קטן

חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$

- תחילה חשבו את p_{even} ו- p_{odd}.
- לאחר מכן חשבו את הפולינום המוקטנים בנקודות המרובעות ע"י הצבה
- מצאו את 4 הנקודות הנדרשות ע"י הנוסחא:

$$p(x) = p_{even}(x^2) + xp_{odd}(x^2)$$

מה שלמעשה עשינו כאן נקרא התמרת פורייה הבדידה (DFT) והיא למעשה הפעולה שאלגוריתם $FFT(p(x), \omega)$ מבצע. כאן מה שלמעשה עשינו הוא הפעלה של $FFT((8, 5, 0, 1), i)$.

השלב האחרון שנותר לנו לממש באלגוריתם

על מנת לחשב את $C = A * B$

השלב האחרון שנותר לנו לממש באלגוריתם

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות (שורשי היחידה מסדר $2n$)

השלב האחרון שנותר לנו לממש באלגוריתם

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות (שורשי היחידה מסדר $2n$)
2. נכפול נקודתית את ערכי A ו-B

השלב האחרון שנותר לנו לממש באלגוריתם

על מנת לחשב את $C = A * B$

1. נחשב את A ו-B ב-$2n$ נקודות (שורשי היחידה מסדר $2n$)
2. נכפול נקודתית את ערכי A ו-B
3. **נחשב את מקדמי הפולינום C מתוך הנקודות**

קסם שלא נסביר

קסם שלא נסביר

- על מנת לחשב את $p(x)$ ב-n נקודות הפעלנו את אלגוריתם

$$FFT((a_0, a_1, \ldots, a_{n-1}), \omega)$$

כאשר $(a_0, a_1, \ldots, a_{n-1})$ הן מקדמי $p(x)$ ו-ω הוא שורש יחידה כלשהו מסדר n.

קסם שלא נסביר

- על מנת לחשב את $p(x)$ ב-n נקודות הפעלנו את אלגוריתם

$$FFT((a_0, a_1, \ldots, a_{n-1}), \omega)$$

כאשר $(a_0, a_1, \ldots, a_{n-1})$ הן מקדמי $p(x)$ ו-ω הוא שורש יחידה כלשהו מסדר n.

- כעת אם אנחנו יודעים את פולינום כלשהו ב-n נקודות שהן שורשי היחידה, הפעלה של:

$$FFT(\cdot, \omega^{-1})$$

משחזרת את מקדמי הפולינום. (לאחר חלוקה ב-n)

קסם שלא נסביר

- על מנת לחשב את $p(x)$ ב-n נקודות הפעלנו את אלגוריתם

$$FFT((a_0, a_1, \ldots, a_{n-1}), \omega)$$

כאשר $(a_0, a_1, \ldots, a_{n-1})$ הן מקדמי $p(x)$ ו-ω הוא שורש יחידה כלשהו מסדר n.

- כעת אם אנחנו יודעים את פולינום כלשהו ב-n נקודות שהן שורשי היחידה, הפעלה של:

$$FFT(\cdot, \omega^{-1})$$

משחזרת את מקדמי הפולינום. (לאחר חלוקה ב-n)

- מי זה ω^{-1}?

הערות

הערות

- שימו לב שזו הסיבה העיקרית לבחירה שלנו להעריך את $p(x)$ בשורשי היחידה.

הערות

- שימו לב שזו הסיבה העיקרית לבחירה שלנו להעריך את $p(x)$ בשורשי היחידה.
- אם היינו מעריכים את $p(x)$ בסתם נקודות הכל היה עובד אך לא היינו מצליחים לשחזר חזרה את המקדמים מתוך הנקודות בשלב האחרון באלגוריתם.

הערות

- שימו לב שזו הסיבה העיקרית לבחירה שלנו להעריך את $p(x)$ בשורשי היחידה.
- אם היינו מעריכים את $p(x)$ בסתם נקודות הכל היה עובד אך לא היינו מצליחים לשחזר חזרה את המקדמים מתוך הנקודות בשלב האחרון באלגוריתם.
- אתם מוזמנים לקרוא בספר את ההוכחה "לקסם" - היא אלגברית לחלוטין
  (מראים שם שהתמרת פורייה היא העתקה לינארית ומוכיחים שהתמרת פורייה עם ω^{-1} היא בדיוק ההעתקה ההפוכה לה.)

תרגיל

חשבו את $FFT(\cdot, \omega^{-1})$ על התוצאה שקיבלתם בתרגיל הקודם.
(תזכורת לתרגיל: חשבו את הפולינום המתאים לקורדינטות הבאות
$p(x) = x^3 + 5x + 8$ ב-4 הנקודות הבאות $(1, i, -1, -i)$)

תרגיל

תרגיל

- נגדיר $P_A = x^2 \quad P_B = 3x + 8$

תרגיל

- נגדיר $P_B = 3x + 8 \quad P_A = x^2$
- חשבו את $C = P_A \cdot P_B$ ע"י הרצת:

תרגיל

- נגדיר $P_B = 3x + 8 \quad P_A = x^2$
- חשבו את $C = P_A \cdot P_B$ ע"י הרצת:

תרגיל

- נגדיר $P_B = 3x + 8 \quad P_A = x^2$
- חשבו את $C = P_A \cdot P_B$ ע"י הרצת:
  - חשבו $FFT_4(A), FFT_4(B)$ ומצאו את הפולינומים ב-4 שורשי היחידה מסדר 4

תרגיל

- נגדיר $P_A = x^2 \quad P_B = 3x + 8$
- חשבו את $C = P_A \cdot P_B$ ע"י הרצת:
  - חשבו $FFT_4(A), FFT_4(B)$ ומצאו את הפולינומים ב-4 שורשי היחידה מסדר 4
  - הכפילו את הערכה של A,B בשורשי היחידה על מנת לקבל הערכה של פולינום C ב4 שורשי היחידה

תרגיל

- נגדיר $P_A = x^2 \quad P_B = 3x + 8$
- חשבו את $C = P_A \cdot P_B$ ע"י הרצת:
  - חשבו $FFT_4(A), FFT_4(B)$ ומצאו את הפולינומים ב-4 שורשי היחידה מסדר 4
  - הכפילו את הערכה של A,B בשורשי היחידה על מנת לקבל הערכה של פולינום C ב4 שורשי היחידה
  - מצאו את מקדמי C ע"י הפעלה של $FFT(\cdot, \omega^{-1})$ על התוצאה מהסעיף הקודם

שאלה מתוך מבחן

שאלה מתוך מבחן

- נתונות שתי קבוצות של n מספרים טבעיים קטנים מ-$16n$

שאלה מתוך מבחן

- נתונות שתי קבוצות של n מספרים טבעיים קטנים מ-$16n$
- $A, B \subseteq \{1, 2, ...16n\}$

שאלה מתוך מבחן

- נתונות שתי קבוצות של n מספרים טבעיים קטנים מ-$16n$
- $A, B \subseteq \{1, 2, \dots 16n\}$
- חשבו את אוסף כל הזוגות

$$\{x + y : x \in A, y \in B\}$$

שאלה מתוך מבחן

- נתונות שתי קבוצות של n מספרים טבעיים קטנים מ-$16n$
- $A, B \subseteq \{1, 2, \dots 16n\}$
- חשבו את אוסף כל הזוגות

$$\{x + y : x \in A, y \in B\}$$

- דוגמא

$$A = \{1, 10\}, \quad B = \{1, 3\} \quad \{2, 4, 11, 13\}$$