אלגוריתמים 2

20 בנובמבר 2015

סיבוכיות של פעולות אריתמטיות

29.10.15

תזכורת: חיבור וחיסור ניתנים לביצוע בזמן $\mathcal{O}(n)$ כאשר n הוא מספר הביטים (ולא גודל המספר). כפל וחילוק ניתנים לחישוב בזמן $\mathcal{O}(n^2)$

חשבון מודולרי

חיבור: $a+b\,(mod\,m)$ כאשר $a,b\in\mathbb{Z}_m$ ו m באורך $n\geq$ ביטים
$0\leq a+b<2m$ ולכן נקבל זמן ריצה

$$\mathcal{O}(n) \quad \ni \quad \begin{cases} a+b & \Leftarrow a+b<m \\ a+b-m & \Leftarrow a+b\geq m \end{cases}$$

כפל: $ab\,(mod\,m)$ אשר $a,b\in\mathbb{Z}_m$ ו m באורך $n\geq$ ביטים
החישוב דורש פעולת כפל + פעולת חילוק עם שארית ובסה"כ זמן ריצה $\mathcal{O}\left(n^2\right)$

חילוק: למעשה חילוק מעל הממשיים משמעותו הכפלה באיבר ההופכי כלומר $a/b\Rightarrow ab^{-1}$
כאשר $b^{-1}b=1$
ב$\mathbb{Z}_m$ לא תמיד קיים הופכי אבל אם m ראשוני ו$0\neq a\in\mathbb{Z}_m$ אזי קיים $a'\in\mathbb{Z}_m$ כך ש $aa'=1(mod\,m)$
במקרה כזה נאמר ש$\mathbb{Z}_m$ הוא לא רק חוג אלא שדה

האלגוריתם של אוקלידס למציאת GCD

נעבור לדון כעת באלגוריתם $gcd(a,b)$ כאשר במהלך היון בה"כ $a\leq b$

טענה: אם $b=0\,mod\,m$ כלומר $a\mid b$ אזי - $gcd(a,b)=a$
אחרת - $gcd(a,b)=gcd(a,a-b)$

נימוק: $c|a\wedge c|a\Rightarrow c|ab$ ומנגד $c|a\wedge c|b-a\Rightarrow c|a+b-a=b$
נחסר אם כך את aמbשוב ושוב עד שנרד מתחת ל-aונקבל את בצד ימין $b\,mod\,a$

מסקנה: $gcd(a,b) = gcd(a,b-ka) = gcd(a, b\;mod\;a)$ עבור k כלשהו ומכאן נקבל אלגוריתם רקורסיבי:

$GCD - Euclid(a,b)$:

- $c = b\;mod\;a$
- אם $c = 0$ - נחזיר a
- אחרת - נחזיר $GCD - Euclid(c,a)$

זמן ריצה - a,b באורך $\geq n$ ביטים

בהתבוננות ראשונית נוכל לשים לב שבכל צעד אחד המספרים קטן ולכן נוכל להסיק שעומק הרקורסיה $\geq max(a,b) \geq 2^n$

טענה: $b\;mod\;a \leq \frac{b}{a}$

הוכחה: נחלק למקרים -

1. $a \leq \frac{b}{2}$ - $b\;mod\;a < a \leq \frac{b}{a}$
2. $a > \frac{b}{2}$ - נקבל כי $b\;mod\;a = b - a < b - \frac{b}{2} = \frac{b}{2}$

אם כך בכל צעד <u>אחד</u> הפרמטרים קטן לפחות בחצי $\Leftarrow$מספר האיטרציות הוא לכל היותר $2log_2 min(a,b)$ ומאחר ו$a,b \leq 2^n$ נקבל $\mathcal{O}(n)$ איטרציות $\Leftarrow$נבצע $\mathcal{O}(n)$ פעמים חילוק עם שארית ולכן סה"כ זמן ריצה $\mathcal{O}(n^3)$

משפט: אם ראשוני ו $0 \neq a \in \mathbb{Z}_m$ אזי קיים $a' \in \mathbb{Z}_m$ כך ש $aa' = 1 \in \mathbb{Z}_m$

למה: הלמה של בזו $(Bézout)$
לכל $a,b \in \mathbb{N}$ קיים $x,y \in \mathbb{Z}$ כך ש:
$xa + yb = GCD(a,b)$

הוכחת המשפט: יהי $0 \neq a \in \mathbb{Z}_m$ כאשר m ראשוני
$GCD(a,m) = 1 \Rightarrow \exists x,y:\; xa + ym = 1 \Rightarrow xa = 1 + (-y)bm \Rightarrow xa = 1(mod\,m)$

הערה: גם אם mפריק אבל $GCD(a,m) = 1$ קיים הופכי לa ב$\mathbb{Z}_m$

הוכחת הלמה: נשנה מעט את הלגוריתם של אוקלידס כך שיחזיר גם x,yשעבורם $xa + yb = GCD(a,b)$
$GCD - Euclid(a,b)$:
$c = b\;mod\;a$ ונשמור את d שעבורו $b = da + c$
אם $c = 0$: נחזיר את צש וגם $x = 1$ $y = 0$
אחרת: נחזיר את $GCD(c,a)$ וגם את $x = y' - dx$ $y = x'$ אותם קיבלנו מהרקורסיה

הסבר: נניח שהקריאה הרקורסיבית החזירה x,y כך ש $x'c + y'a = GCD(c,a) = GCD(a,b$
בפעולה $b\;mod\;a$ קיבלנו c,d כך ש $b = da + c$
כלומר $x'c + y'a = x'(b - da) + y'a = x'b + (y' - dx')a$ כנדרש

סבוכיות: $\mathcal{O}\left(n^3\right)$

בדיקת ראשוניות

חישוב חזקה בחשבון מודולרי

a,b,m באורך $\geq m$ ביטים
רוצים לחשב את $a^b \, mod \, m$

הבעיה: a^b הוא מספר באורך $\approx ab$ ביטים כלומר $\mathcal{O}\left(n2^n\right)$

רעיון: נבצע $mod \, m$ לאחר כל כפל. אלא שזה עדיין לא מספיק משום שאנחנו נדרשים לבצע b פעולות/איטרציות כאשר $b = \mathcal{O}\left(2^n\right)$

טריק נפוץ ושימושי: נחשב את הסדרה $a \, mod \, m, \; a^2 \, mod \, m, \; a^4 \, mod \, m, \; \ldots, a^{2^n} \, mod \, m$
- סדרה בת n איברים
בשביל לחשב כל איבר בסדרה פשוט נעלה את קודמו בריבוע. נשים לב שמתכונות החשבון המודולרי תוצאת ה mod תהיה זהה גם אם נבצע אותה אחרי כל העלאה בריבוע.
נקבל שלחישוב כל איבר נזדקק לפעולת כפל + פעולת mod (ששוות ערך לחילוק עם שארית) כלומר $\mathcal{O}\left(n^2\right)$ פעולות
ולכן בסך הכל עבור ככל הסדרה נקבל $\mathcal{O}\left(n^3\right)$
כעת נוכל לפרק את החזקה (בעזרת הייצוג הבינארי שלה) לסכום של חזקות של 2 כלומר $b = 2^{x_1} + 2^{x_2} + \ldots$, נקבל, אם כך, כפל של חזקות $a^b = a^{s^{x_1}} a^{2^{x_2}} \ldots$
גם כאן נכניס את פעולת ה mod פנימה ונקבל: $b = \sum 2^{x_k} \Rightarrow a^b \; mod \; m = \prod_k (a^{2^{x_k}} \; mod \, m)$

זמן ריצה: עיבוד ראשוני - $\mathcal{O}\left(n^3\right)$ עבור חישוב הסדרה
בכל שלב עבור כל x_k נכפיל - $(\prod_{j=1}^{k-1} a^{2^{x_j}} \; mod \, m)(a^{2^{x_k}} \; mod \, m) \; mod \; m$ - כאשר הכופל השמאלי הוא מה שחושב עד כה והימני הוא החישוב המבוקש
ולכן מדובר בכל שלב בכפל + $mod \Leftarrow$ סה"כ $\mathcal{O}\left(n^3\right)$

$PRIMES$

ישנן שתי בעיות קרובות אבל שונות מאוד בתחום של ראשוניות:

1. בדיקת ראשוניות $(PRIMES)$ - בהינתן $m \in \mathbb{N}$ האם הוא ראשוני?
2. פירוק לגורמים $(FACTORING)$ - בהינתן $m \in \mathbb{N}$ פריק, מצא גורם של m
בהנתן אלגוריתם שפותר את בעיה 2 נוכל למצוא ע"י את כל הגורמים של m על ידי חילוק בגורם שמצאנו והפעלה חוזרת

בעיה 1 היא בעיה קלה - שיערו שזה כך ואכן בשנת 2002 הוכח שהיא בP

בעיה 2 לעומת זאת נחשבת בעיה קשה - לא ידוע על אלגוריתם שפותר אותה בזמן סביר

1.11.15

היסטוריה

1976: אלגוריתם של $Miller$ דטרמיניסטי ופולינומי
$Miller$ הוכיח שהאלגוריתם נכון אם השערת רימן המוכללת נכונה

1977: אלגוריתם של $Solovag-Starassen$ רנדומי, פולינומי, נכון ללא הנחות
הראו ש $PRIMES\in CO-RP$
$CO-RP$ ־ אלגוריתמים בעלי אפשרות רנדומית לטעות חד־צדדית.
כלומר במקרה שלנו ־ אם m ראשוני ־ האלגוריתם יחזיר "כן" תמיד, אם הוא פריק ־ האלגוריתם יחזיר "לא" בהסתברות $\le\frac{1}{2}$
אם חוזרים k פעמים על האלגוריתם על m נתון, ההסתברות שנחזיר בכל הפעמים "כן" כאשר למעשה m פריק היא $\le\left(\frac{1}{2}\right)^k$

1980: $Miller-Rabin$ אלגוריתם ב $C-RP$ (כלומר עם שגיאה הסתברותית חד צדדית), יעיל יותר (דרגת הפולינום נמוכה יותר), נכון ללא הנחות

1992: $Adelman-Hung$ אלגוריתם ZPP כלומר רנדומי במובן הזה שהוא תמיד מחזיר תשובה נכונה ותוחלת זמן הריצה היא פולינומית
הערה: נניח שתוחלת זמן הריצה n^c נקבל מאי־שיוויון מרקוב $Pr\left[run-time\ge 2n^c\right]\le\frac{1}{2}$ ולכן אם נריץ את האלגוריתם k פעמים כל פעם במשך $2n^c$ צעדים ההסתברות שאף ריצה לא תעצור בזמן הזה היא $\le\left(\frac{1}{2}\right)^k$

2001: $Agravant-Kayst-Saysera$ הוכיחו ש $PRIMES\in P$

מציאת מספר ראשוני

הרעיון הכללי: נגריל מספר באורך m ביטים ונריץ אלגוריתם לבדיקת ראשוניות, אם התשובה היא "כן" נחזיר את m.

משפט המספרים הראשוניים: נגדיר $\pi(x)=\left|\{p|p\le x,\ p\,is\,prime\}\right|$ אזי

$$\pi(x)=(1+o(1))\frac{x}{ln\,(x)}$$

ומכאן שבין x ל$2x$ יש $(1+o(1))\frac{x}{ln(x)}$ ראשוניים

כלומר אם נגריל מספר שלם $2^n\le m\le 2^{n+1}$ נקבל ש

$$Pr\left[m\ is\ prime\right]=\frac{(1+o(1))\frac{2^n}{ln(2^n)}}{2^n}=(1+o(1))\frac{1}{nln\,(2)}$$

אם נבצע kn חזרות ההסתברות להצלחה באחת מהן היא

$$1-Pr\left[failor\right]=1-\left(1-\frac{1-o\,(1)}{nln2}\right)^{kn}\ge 1-\left(e^{-\frac{1-o(1)}{nln2}}\right)^{kn}=1-\left(e^{-\frac{1-o(1)}{ln2}}\right)^{k}>1-\left(\frac{1}{4}\right)^k$$

השערה: השערת $Cramer$ ־ הפער המקסימלי בין שני ראשונים עוקבים באורך n ביים הוא $\mathcal{O}\left(n^2\right)$
התוצאה הכי טובה בדרך להוכחת ההשערה היא שפער לא גדול מ $\approx\frac{1}{n}2^{\frac{n}{2}}$

אלגוריתם $CO-RP$ לבדיקת ראשוניות

עד פשוט לפריקות: m פריק $\Leftarrow$ קיים $0<a<m$ כך ש $GCD(a,m)\neq 1$

דוגמה: אם $m=pq$ כאשר p,q ראשוניים באורך n $\left(2^{2n}\approx m,\ 2^n\approx p,q\right)$ כמה עדים יהיו?

$$\begin{cases}\text{p,2p,...}(q-1)p\\ q,2q,...,(p-1)q\end{cases} p+q+2 \text{ עדים מתוך } m$$

כלומר אם נגריל ההסתברות שנפגע בעד היא בערך $2\frac{2^n}{2^{2n}}$ $\mathcal{O}\left(\frac{1}{2^n}\right)$ - לא יעיל!

משפט: משפט פרמה הקטן

אם p ראשוני אזי לכל $1<a<p-1$ מתקיים $a^{p-1}\equiv 1\,mod\,p$

הוכחה: נבחר $1<a<p-1$ ונסתכל על הקבוצה $A=\{ai\,mod\,p\mid i=1...p-1\}$

$\mathbb{Z}_p$ שדה $\Leftarrow$ אם $i,j\in\mathbb{Z}_p$ כך ש $\Leftarrow$ $(i-j)a\bar{a}\equiv 0\,mod\,p$ $\Leftarrow$ $i\equiv j\,mod\,p$

$(i-j)a\equiv 0 \Leftarrow ia\equiv ja$

מנימוק דומה ניתן להראות שכל אברי הקבוצה שונים מ0 ולכן למעשה אברי A הם כל המספרים $1,...,p-1$ בפרמוטציה כלשהי

ומכאן

$$0\overset{*}{\neq}\neq\prod_{i=1}^{p-1}i=\prod_{i=1}^{p-1}ai\,mod\,p$$

* בשדה אין כופלי אפס ולכן מכפלה של אברים שאינם אפס בהכרח שונה מאפס

מאחר ואנחנו בשדה לכל איבר קיים הופכי ולכן נוכל להכפיל ב $\left(\prod_{i=1}^{p-1}i\right)^{-1}$

$$a^{p-1}=\left(\prod_{i=1}^{p-1}i\right)\left(\prod_{i=1}^{p-1}i\right)^{-1}\equiv 1\,mod\,p$$

ציינו מקודם שאם m פריק קיים $0<a<m$ כך ש $GCD(a,m)\neq 1$ ובפרט $a^{m-1}\neq 1\,mod\,m$ כי אם $c|a,m$ $\Leftarrow$ $c|a^k-jm$כלומר חזקות של a נקבל תמיד מספר שמחלק את c (מודולו m)

שאלה: הטענה יכולה חד משמעית לשלול ראשוניות (אם היא לא מתקיימת עבור a כלשהו) אבל מה יקרה אם m למעשה פריק? אז יתכן מצב שבו קיים a שיקיים את השקילות $a^{m-1}\equiv 1\,mod\,m$. נרצה לוודא שאם המספר פריק בדיקת השקילות של משפט פרמה תכשל בסבירות גבוה.

אם כך נשאל - מה קורה אם קיים a כך ש $GCD(a,m)=1$ ובנוסף a הוא עד לפריקות על פי פרמה כלומר $a^{m-1}\not\equiv 1\,mod\,m$. או במילים אחרות a אמנם זר ל m ולכן לא יכול להפריך את הראשוניות של m באופן הנאיבי שהצענו אבל מצד שני הוא כן מפריך את הראשוניות על פי פרמה?

למה: אם קיים a כך ש $GCD(a,m)=1$ ובנוסף $a^{m-1}\not\equiv 1\,mod\,m$

אזי לפחות חצי מהמספרים $b\in\{1,..,m-1\}$ מקיימים גם $b^{m-1}\not\equiv 1\,mod\,m$

הוכחה: נגדיר $X=\left\{1\leq x\leq m-1|x^{m-1}\not\equiv 1\,mod\,m\right\}$ ונסמן את שאר האיברים בטווח $Y=\left\{1\leq y\leq m-1|y^{m-1}\equiv 1\,mod\,m\right\}$

נראה ש $|X| < |Y|$ על ידי המיפוי החד־חד־ערכי מ Y ל־X הבא:

$$y \in Y \mapsto ay \, mod \, m$$

נראה תחילה שזו אכן מעתיקה איברים מ Y ל־ X

$$(ay)^{m-1} \equiv a^{m-1}y^{m-1} \equiv a^{m-1} \not\equiv 1 \, mod \, m \Rightarrow ay \in X$$

הראנו בעבר שגם אם $\mathbb{Z}_m$לא שדה עבור a כך ש $GCD(a,m) = 1$ קיים הופכי ב Z_m
נשתמש בעובדה זו כדי להראות את החד־חד־ערכיות של ההעתקה שהגדרנו

$$ay \equiv az \, mod \, m \Rightarrow a^{-1}ay \equiv a^{-1}az \, mod \, m \Rightarrow y \equiv z \, mod \, m$$

מסקנה: אם קיים a שהינו עד שסותר את משפט פרמה הקטן אבל הוא זק ל־m אזי יש "הרבה" כאלה (יותר מ$\frac{1}{2}$) עדים כאלה.
ולכן נוכל להגדיר את האלגוריתם הבא:

$: Not - Quite - Miller - Rabin(m)$

- נגריל $a \in \{1, ..., m-1\}$ ונבדוק
  - אם $a^{m-1} \equiv 1 \, mod \, m$: נחזיר "כן"
  - אחרת : נחזיר "לא"

אם m ראשוני אז על פי משפט פרמה הקטן תנאי הבדיקה יהיה תמיד חיובי ולכן תמיד נזהה נכון ונחזיר "כן"

אם m פריק אז או שתנאי הבדיקה של משפט פרמה הקטן יכשל ונזהה נכון את m כפריק או שבמקרה ניפול על $a \in Y$ כלומר $a^{m-1} \equiv 1 \, mod \, m$ ואז נטעה ונחשוב ש m ראשוני. אבל הראנו שהסיכוי שהאפשרות השניה תקרה היא קטנה מ $\frac{1}{2}$ כלומר במקרה ש m פריק נחזיר תשובה נכונה בהסתברות $\leq \frac{1}{2}$.