1

אוטומטים ושפות פורמליות 2

נושא 1 - משפט נרוד

א) הקדמה

עד כה למדנו רק כלי אחד לבחון האם שפה היא רגולרית או לא באמצעות למת הניפוח.

אמנם למת הניפוח אינה תנאי מספיק שכן רק אומרת שכל שפה שלא מקיימת את התנאים אינה רגולרית, אך זה אינו אם ורק אם. יכול להיות שפה לא רגולרית שמקיימת את התנאים.*

*כא הבאנו את $L=\{a^i b^j c^k ...\}$

בפרק זה נלמד כלי נוסף "משפט נרוד" שמספק תנאים אם ורק אם. אמנם כדי להבין אותו יש להסביר כמה מושגים מלוגיקה.

ב) יחס שקילות

יחס שקילות R על קבוצה A הוא יחס בינארי, כלומר $R\subseteq A\times A$, המקיים שלושה תנאים:

(1) רפלקסיביות: לכל $x\in A$ (x,x) שייך ליחס. בסימון מקובל $R(x,x)$ או xRx.

(2) סימטריות: לכל $x,y\in A$ אם $R(x,y)$ אזי גם $R(y,x)$.

(3) טרנזיטיביות: לכל $x,y,z\in A$ אם $R(x,y)$ וגם $R(y,z)$ אזי גם $R(x,z)$.

כל יחס שקילות R על A, משרה חלוקה יחידה של A למחלקות שקילות $A_1,A_2,...$ המקיימות:

(1) המחלקות אינן ריקות ואיחודן שווה ל-A.

(2) לכל $x\in A_i$ ולכל $y\in A_j$, $(x,y)\in R$ אם ורק אם $i=j$. במילים אחרות, כל שני איברים מאותה מחלקת שקילות ביחס וכל שני איברים שאינם מאותה מחלקה לא ביחס.

המשמעות היא שכל מחלקות השקילות זרות וכל $x\in A$ שייך למחלקת שקילות אחת בדיוק. לכן כדי לסמן מחלקת שקילות ניתן לקחת כל איבר x בתוכה שישמש נציג, בסימון $[x]$. את מספר מחלקות השקילות שמשרה R נסמן $index(R)$, יכול להיות גם אינסופי.

ניתן לייצג מחלקות שקילות באמצעות גרפים, כך שכל רכיב קשירות הוא מחלקה נפרדת וכל רכיב קשירות הוא קליקה (גרף מלא).

ג) יחס עידון

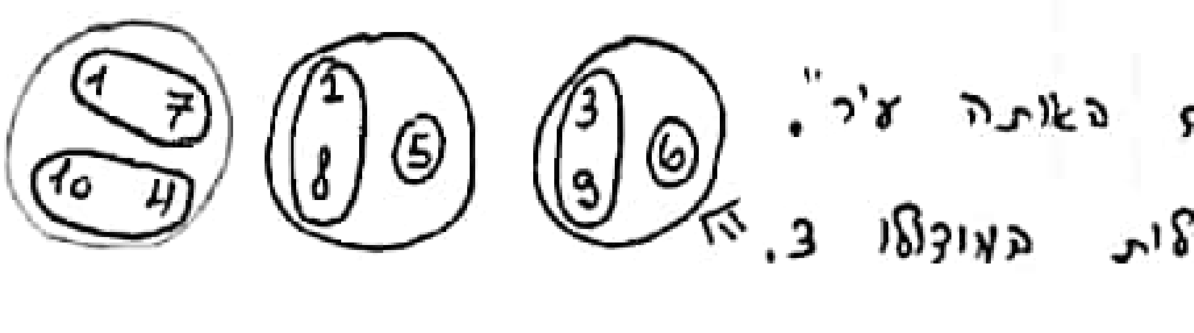
נאמר כי יחס שקילות R_1 "מעדן" יחס שקילות R_2 אם ורק אם שניהם מעל אותה הקבוצה, וגם לכל $x,y\in A$ אם $(x,y)\in R_1$ אזי גם $(x,y)\in R_2$. במילים אחרות, כל מחלקת שקילות ב-R_1 מוכלת* ב-R_2.

*במחלקת שקילות

-מסקנה חשובה: מספר מחלקות השקילות של R_1 תמיד גדול או שווה ל-R_2. $index(R_1)\geq index(R_2)$

דוגמאות: (1) היחס "גרים באותו בית" מעדן את היחס "גרים באותה עיר".

(2) היחס שקילות במודולו 6 מעדן את היחס שקילות במודולו 3.



3) יחס אינווריאנטי מימין

יחס שקילות R מעל Σ^* יקרא אינווריאנטי מימין אם לכל $x,y,z\in\Sigma^*$, אם $(x,y)\in R$ אזי גם $(xz,yz)\in R$. במילים אחרות, אם x,y באותה מחלקת שקילות, אזי לכל סיפא z גם xz ו-yz באותה מחלקת שקילות. לא בהכרח באותה מחלקת שקילות של x ו-y.

אם $(x,y)\in R$ אזי $\Downarrow$ $\forall z\in\Sigma^*\ (xz,yz)\in R$

דוגמא: היחס $R=\{(x,y): |x|=|y|\}$ אינווריאנטי מימין שכן לכל $z\in\Sigma^*$ $|xz|=|x|+|z|=|y|+|z|=|yz|$.

ה) היחס $\tilde{R}_L$

תהי שפה $L\subseteq\Sigma^*$. היחס $\tilde{R}_L$ של שפה L הוא יחס בינארי מעל Σ^* $(\tilde{R}_L\subseteq\Sigma^*\times\Sigma^*)$, המוגדר כך: $\tilde{R}_L=\{(x,y)\in{\Sigma^*}^2: x\in L \iff y\in L\}$. כלומר $\tilde{R}_L$ הוא יחס של זוגות מילים ב-Σ^* ששייכות או לא שייכות ביחד ל-L.

היחס $\tilde{R}_L$ הוא יחס שקילות, וקל לראות זאת. מחלקות השקילות שלו הן בדיוק L ו-$\bar{L}$.

ו) היחס R_L

תהי שפה $L\subseteq\Sigma^*$. היחס R_L של שפה L הוא יחס בינארי מעל Σ^* $(R_L\subseteq\Sigma^*\times\Sigma^*)$ המוגדר כך: $R_L=\{(x,y)\in{\Sigma^*}^2: \forall z\in\Sigma^*, xz\in L \iff yz\in L\}$. במילים, זוג מילים x,y נמצאים ביחס אם ורק אם לא קיימת סיפא z המפרידה בין x ל-y במובן ש-$xz\in L$ אך $yz\notin L$, או להיפך.

משפטים:

1) משפט: לכל שפה L, R_L הוא יחס שקילות.

הוכחה: רפלקסיביות - תהי $x\in\Sigma^*$. לכל $z\in\Sigma^*$ מתקיים $xz\in L \iff xz\in L$ כי זו אותה מילה.

סימטריות - יהיו $(x,y)\in\Sigma^*$. נניח $(x,y)\in R_L$ אזי לכל $z\in\Sigma^*$ $xz\in L \iff yz\in L$. כיוון שהאופרטור $\iff$ מתקיים גם $yz\in L \iff xz\in L$, ולכן גם $(y,x)\in R_L$.

טרנזיטיביות - יהיו $x,y,z\in\Sigma^*$. נניח $(x,y)\in R_L$ וגם $(y,z)\in R_L$. אזי לכל $u\in\Sigma^*$ נובע כי גם $xu\in L \iff yu\in L$ וגם $yu\in L \iff zu\in L$. לכן גם $xu\in L \iff zu\in L$, ולכן $(x,z)\in R_L$.

2) משפט: היחס R_L אינווריאנטי מימין.

הוכחה: הוכחנו ש-R_L יחס שקילות מעל Σ^*. נניח כי $(x,y)\in R_L$ ונראה כי לכל $z\in\Sigma^*$ $(xz,yz)\in R_L$.

תהי $u\in\Sigma^*$. לפי תכונת R_L עבור הסיפא zu מתקיים $x(zu)\in L \iff y(zu)\in L$. מאסוציאטיביות של שרשור מחרוזות נובע כי $(xz)u\in L \iff (yz)u\in L$. כיוון ש-$u$ מחרוזת כלשהי נסיק כי גם אין סיפא שמפרידה בין xz ל-yz, ולכן $(xz,yz)\in R_L$. נובע מכך ש-R_L אינווריאנטי מימין.

③

3) משפט: היחס R_L מעדן את היחס $\tilde{R}_L$

הוכחה: כבר הראנו ששניהם יחסי שקילות מעל Σ^*. נניח כי עבור $x,y\in\Sigma^*$ מתקיים $(x,y)\in R_L$.
אז לכל $z\in\Sigma^*$ $xz\in L \Leftrightarrow yz\in L$. בפרט עבור $z=\varepsilon$ נקבל $x\in L\Leftrightarrow y\in L$. ולכן $(x,y)\in\tilde{R}_L$.

ב) היחס R_A

יהי A אס"ד המקבל שפה $L(A)\in\Sigma^*$. נניח כי מצבי האוטומט A הם $Q=\{q_0,q_1,\dots,q_n\}$, כאשר q_0 מצב התחלתי. היחס R_A על אס"ד A הוא יחס בינארי מעל Σ^* ($R_A\subseteq\Sigma^*\times\Sigma^*$), המוגדר כך: $R_A=\{(x,y)\in\Sigma^{*2}: \delta(q_0,x)=\delta(q_0,y)\}$. כלומר שתי מילים שייכות ליחס אם A מגיע לאותו מצב בחישוב על שתיהן.

משפטים:

1) משפט: לכל אס"ד A, היחס R_A: הוא יחס שקילות

הוכחה: טריוויאלי ואין צורך להאריך.

2) משפט: R_A מחלק את Σ^* למחלקות שקילות $S_0,S_1,\dots,S_n$ בהתאם למצבים ב-A. כלומר כל מחלקת שקילות S_i מכילה את כל המילים שמגיעות למצב q_i. $S_i=\{x\in\Sigma^*: \delta(q_0,x)=q_i\}$.

הוכחה: חלוקה זו תקינה שכן כל מילה ב-Σ^* מגיעה למצב כלשהו באוטומט, ולכן זוהי חלוקה שלמה של Σ^*. בנוסף אין מחלקה ריקה שכן כל מצב מסתיימת בו לפחות מילה אחת אחרת לא היה באוטומט. וכן מהגדרת R_A נובע כי כל שני מילים שקולות אם ורק אם מגיעות לאותו המצב באוטומט.

מסקנות: ① השפה המתקבלת ע"י האוטומט, $L(A)$, היא איחוד מחלקות השקילות של המצבים המקבלים. $L(A)=\bigcup_{q\in F} q$.

② מספר מחלקות השקילות כמספר המצבים ולכן $index(R_A)<\infty$.

3) משפט: היחס R_A אינוריאנטי מימין

הוכחה: הוכחנו ש-R_A יחס שקילות על Σ^*. נניח כי $(x,y)\in R_A$. לכל $z\in\Sigma^*$ מתקיימת המשוואה הבאה: $\delta(q_0,xz)\underset{\text{תכונת שרשור}}{=}\delta(\delta(q_0,x),z)\underset{\text{יחס } R_A}{=}\delta(\delta(q_0,y),z)\underset{\text{תכונת שרשור}}{=}\delta(q_0,yz)$. ומכאן שבהכרח $(xz,yz)\in R_A$, ולכן אינוריאנטי מימין.

4) משפט: היחס R_A מעדן את $\tilde{R}_{L(A)}$.

הוכחה: כבר הראנו ששניהם יחסי שקילות מעל Σ^*, נניח כי $(x,y)\in R_A$, אז מתקיים $q=\delta(q_0,x)=\delta(q_0,y)$.
כלומר שניהם מסתיימים באותו המצב q. לכן אם q מצב מקבל x ו-y יתקבלו, אך אם לא הם לא יתקבלו, $x,y\in L(A)\Leftrightarrow q\in F$. המסקנה היא שהם מתקבלים או לא מתקבלים ביחד ולכן $(x,y)\in\tilde{R}_{L(A)}$.

4

5) משפט: היחס R_A מעדן את היחס $R_{L(A)}$.

הוכחה: שניהם יחסי שקילות מעל Σ^* כפי שהוכח לעיל. נניח $(x,y)\in R_A$, אזי לכל $z\in\Sigma^*$ מתקיים $\delta(q_0,xz)\underset{\text{שרשור}}{=}\delta(\delta(q_0,x),z)\underset{R_A \text{ יחס}}{=}\delta(\delta(q_0,y),z)\underset{\text{שרשור}}{=}\delta(q_0,yz)$, כלומר xz ו-yz מסתיימים באותו מצב q כלשהו. אם q מצב מקבל אזי xz ו-yz שייכים ל-$L(A)$ ואם q לא מצב מקבל אז הם לא שייכים, לכן שניהם מתקבלים או לא מתקבלים ביחד, $xz\in L(A) \Leftrightarrow yz\in L(A)$, ומכאן $(x,z)\in R_{L(A)}$.

ח) משפט האפיון של R_L

היחס R_L על שפה L הוא יחס שקילות מעל Σ^* המקיים את שלושת המשפטים הבאים:

(1) R_L אינווריאנטי מימין.

(2) R_L מעדן את $\tilde{R}_L$.

(3) כל יחס שקילות בינארי $R\subseteq\Sigma^*\times\Sigma^*$ המקיים את (1) ו-(2) <u>מעדן את R_L</u>, מכיוון שכבר הוכחנו ש-R_L מקיים את (1) ו-(2), המשמעות היא ש-R_L הוא יחס השקילות עם המספר הקטן ביותר של מחלקות שקילות המקיים את (1) ו-(2), כלומר אשר את החלוקה הכי גסה מבין כל יחסי השקילות המקיימים אותם.

הוכחה עבור (3): יהי R יחס שקילות בינארי מעל Σ^* המקיים את (1) ו-(2). נניח $(x,y)\in R$. מכיוון ש-R אינווריאנטי מימין לכל $z\in\Sigma^*$ מתקיים $(xz,yz)\in R$. כיוון ש-R גם מעדן את $\tilde{R}_L$ מתקיים $(xz,yz)\in\tilde{R}_L$. מהגדרת $\tilde{R}_L$ נובע כי $xz\in L\Leftrightarrow yz\in L$. נמצא כי עבור כל $z\in\Sigma^*$, $xz\in L\Leftrightarrow yz\in L$, ולכן $(x,y)\in R_L$. מ.ש.ל.

בנוסף ליחס שקילות המקיים (1) ו-(2) וגם מעדן את R_L היא R_A, שהראנו בסעיף קודם שמקיים את כל שלושת התנאים.

ט) <u>משפט נרוד</u>

<u>משפט:</u> תהי $L\subseteq\Sigma^*$ שפה. L היא רגולרית אם ורק אם $index(R_L)<\infty$, כלומר ליחס R_L יש מספר סופי של מחלקות שקילות.

<u>הוכחה: כיוון 1</u> - נניח L רגולרית ונוכיח $index(R_L)<\infty$, אם L רגולרית יש אוטומט A שמקבל אותה $L=L(A)$. היחס R_A של A מעדן את R_L. לכן מספר מחלקות השקילות ב-R_A לפחות כמו מספר מחלקות השקילות ב-R_L. ומכיוון שמספר מחלקות השקילות ב-R_A כמספר המצבים שהוא סופי, גם מספר מחלקות השקילות ב-R_L סופי. $index(R_L)\le index(R_A)=|Q|<\infty$.

5

כיוון 2 - תהי L שפה כך שמתקיים $index(R_L)<\infty$, נוכיח כי L רגולרית באמצעות בנייה של אס"ד A_L שיקבל את L (הוכחה קונסטרוקטיבית). נגדיר אס"ד $A_L=(Q,q_0,\Sigma,F,\delta)$.

Q - נגדיר את קבוצת המצבים ב-A בהתאמה למחלקות השקילות ב-R_L. כל מצב q_i יסמן את כל המילים במחלקת השקילות S_i. מספר המחלקות סופי ולכן גם מספר המצבים. נוכל לייצג את q_i באמצעות כל איבר מ-S_i שישמש נציג הקבוצה $q_i=[x_i]$. לסיכום $Q=\{[x]: x\in\Sigma^*\}$.

q_0 - המצב ההתחלתי מייצג את מחלקת השקילות שמכילה את ε, נניח ε נציג המחלקה, $[\varepsilon]=q_0$.

Σ - כמו ה-Σ של L.

F - נגדיר את המצבים המקבלים להיות כל המצבים שמייצגים מחלקות שקילות המכילות מילים השייכות ל-L. $F=\{q_i=[x_i]: x_i\in L\}$.

δ - עבור כל מצב $q_i=[x_i]\in Q$ ואות $a\in\Sigma$, נגדיר פונקציית מעברים $\delta(q_i,a)=\delta([x_i],a)=[x_ia]=[x_j]=q_j$.
כלומר עבור מצב q_i שהנציג שלו $[x_i]$ ואות a, δ מעבירה למצב המייצג את מחלקת השקילות של האיבר $[x_ia]$, שהוא מצב q_j. נשים לב ש-q_i לא בהכרח שונה מ-q_j.

<u>נוכיח ש-A מוגדר היטב:</u>

הבעיה היחידה שצריך לחשוש ממנה היא ש-F ו-δ תלויים בנציג שבחרנו לכל מחלקת שקילות. נראה שאין לחשוש מכך.
נתבונן במצב q_i המקבל את מחלקת השקילות וכן שני נציגים אפשריים x_i ו-y_i, כלומר $x_i,y_i\in S_i$.
כיוון ששניהם באותה מחלקת שקילות $(x_i,y_i)\in R_L$.
עבור F, כיוון ש-R_L מעדן את $\tilde{R}_L$ אזי $y_i\in L \Leftrightarrow x_i\in L$, לכן שייכות q_i ל-F אינה תלויה בבחירת הנציג.
עבור δ, כיוון ש-R_L אינווריאנטי מימין לכל $a\in\Sigma$ גם $(x_ia,y_ia)\in R_L$, כלומר x_ia ו-y_ia שייכים לאותה מחלקת שקילות. לכן המעבר מ-q_i עבור הקלט a אינו תלוי בנציג המחלקה $\delta(q_i,a)=[x_ia]=[y_ia]$.

<u>טענת עזר</u>: תהי $x\in\Sigma^*$ מילה אזי מתקיים $\delta(q_0,x)=[x]$. כלומר חישוב המילה ב-A_L מוביל למחלקת השקילות שלה.
הוכחה: באינדוקציה על אורך המילה |x|.
בסיס- עבור |x|=0 אזי x=ε, ולכן q_0 מהגדרת q_0. נובע כי $\delta(q_0,\varepsilon)=q_0=[\varepsilon]$.
צעד- נניח שהטענה נכונה עבור |x|=i נוכיח עבור i+1. עבור $a\in\Sigma$ נגדיר y=xa. נשים לב כי מתקיים:

$$\delta(q_0,y)\underset{\text{הגדרת } y}{=}\delta(q_0,xa)\underset{\text{שרשור}}{=}\delta(\delta(q_0,x),a)\underset{\text{הנחת האינדוקציה}}{=}\delta([x],a)\underset{\text{הגדרת } \delta}{=}[xa]\underset{\text{הגדרת } y}{=}[y]$$

<u>נוכיח $L=L(A_L)$:</u>

כיוון 1 - תהי מילה $x\in L$, אזי מתקיים: $\delta(q_0,x)\underset{\text{טענת עזר}}{=}[x]\underset{\text{הגדרת } F}{\in}F$. ולכן $x\in L(A_L)$.

כיוון 2- תהי מילה $x\in L(A_L)$, אזי מתקיים: $\delta(q_0,x)\underset{\text{טענת עזר}}{=}[x]\in F$. מהגדרת F נובע שמחלקת השקילות [x] מתקבלת בשפה L. כיוון ש-$x\in[x]$ מהגדרת δ, נקבל $x\in L$

6

י) הוכחת אי רגולריות באמצעות נרוד

עבור שפה $L\subseteq\Sigma^*$, כדי להוכיח שאינה רגולרית יש למצוא תת קבוצה B אינסופית של מילים שונות ב-Σ^*, ולהראות שכל זוג מילים $p\neq q$ המוכלים ב-B אזי (a,b) אינו קיים R_L, $(a,b)\notin R_L$. אם הצלחנו למצוא B כזאת אזי הוכחנו של-R_L יש $|B|$ מחלקות שקילות. כיוון ש-B אינסופית $index(R_L)>\infty$, לפי משפט נרוד L לא רגולרית.

דוגמאות:

(1) עבור השפה $L=\{a^nb^n : n\in\mathbb{N}\}$ נגדיר את הקבוצה האינסופית $B=\{a^n : n\in\mathbb{N}\}$. עבור כל שני מילים $a^i,a^j\in B$ כאשר $i\neq j$, נבחר $z=b^i$ עבורה $a^ib^i\in L$ אך $a^jb^i\notin L$. לכן מצאנו סיפא מפרידה בין כל שני מילים, $(a^i,a^j)\notin R_L$. כתוצאה מכך $index(R_L)>\infty$ ולכן L לא רגולרית.

(2) עבור השפה $L=\{a^ib^jc^j : i\geq 1, j\geq 0\}\cup\{b^ic^j : i,j\geq 0\}$ נגדיר את הקבוצה האינסופית $B=\{ab^i : i\geq 0\}$.
עבור כל שני מילים $ab^i,ab^j\in B$ כאשר $i\neq j$ נבחר $z=c^i$ עבורה $ab^ic^i\in L$ אך $ab^jc^i\notin L$.
לכן z סיפא מפרידה בין כל שני מילים ב-B, ומתקיים $(ab^i,ab^j)\notin R_L$. מסקנה L לא רגולרית.

יא) הוכחת רגולריות באמצעות נרוד

עבור שפה $L\subseteq\Sigma^*$ כדי להוכיח שהיא רגולרית יש להראות שמספר מחלקות השקילות של R_L סופי, $index(R_L)<\infty$. לשם כך יש להציג חלוקה לקבוצות לא ריקות של Σ^*, כך שכל קבוצה מכילה מילים שהם שקולות ב-R_L, וכל שני מילים מקבוצות שונות אינן ב-R_L.
אם הצלחנו להוכיח זאת, אזי לפי משפט נרוד L רגולרית.

דוגמא: עבור השפה $L=\{w\in\{a,b\}^* : |w|\equiv 0 \pmod 2\}$, המכילה את כל המילים מעל $(a,b)^*$ באורך זוגי.
ב-R_L יש שתי מחלקות שקילות הלבד $S_0=\{w : |w|\equiv 0 \pmod 2\}$, $S_1=\{w : |w|\equiv 1 \pmod 2\}$. כלומר S_0 מילים שאורכם זוגי, ו-S_1 מילים שאורכם אי-זוגי. כיוון שזוהי חלוקה לא ריקה של $(a,b)^*$, ורק אם 2 מילים מאותה מחלקה הן ב-R_L, זוהי אכן חלוקה למחלקות שקילות של R_L.
כיוון ש-$index(R_L)<\infty$ L היא שפה רגולרית.

יב) מינימיזציה של DFA.

עבור כל אוטומט A המקבל את השפה L, הוכחנו כי R_A מעדן את R_L. כתוצאה מכך מספר מחלקות השקילות ב-R_A תמיד גדול או שווה למספר מחלקות השקילות ב-R_L. בנוסף, יכול להיות כי ב-A ישנם מצבים שאינם ישיגים, לכן מספר המצבים ב-A תמיד גדול או שווה למספר מחלקות השקילות ב-R_A. משילוב שני הטענות לעיל נקבל כי לכל אוטומט A ושפה L מתקיים*: $|Q_A|\geq index(R_A)\geq index(R_L)$
*כאשר $L=L(A)$

בס"ד

7

מאי-שוויון זה נוכל להסיק כי בכל אוטומט A מספר המצבים המינימלי האפשרי הוא כמספר מחלקות השקילות ב-R_L, עבור $L=L(A)$. ואכן בהוכחת הכיוון השני של נרוד ראינו שעבור כל שפה רגולרית L ניתן לבנות אוטומט A_L שמספר המצבים בו בדיוק $index(R_L)$.

בעל־רת נתון זה נוכל לקבוע עבור כל אוטומט A אם הוא מינימלי, וזאת כאשר: $index(R_{L(A)})=|Q_A|$.

אמנם נוכל לעשות אף יותר מכך. נוכל להגות אלגוריתם בזמן ריצה פולינומי שמקבל כקלט אס"ד A ומחזיר אס"ד A', כך $L(A')=L(A)\cdot e$ והוא מינימלי עבור השפה $L(A)$. דוגמה לאלגוריתם כזה היא אלגוריתם Moore.

יג) <u>אלגוריתם Moore</u>

קלט: אס"ד $A=(Q,q_0,\Sigma,F,\delta)$

פלט: אס"ד $A'=(Q',q_0',\Sigma,F',\delta')$, כך $L(A')=L(A)\cdot e$ והוא מינימלי עבור השפה $L(A)$.

שלבי האלגוריתם:

(1) נסלק את כל המצבים הלא ישיגים מ-q_0 ב-A. ניתן לעשות זאת באמצעות BFS או DFS.

(2) נאתחל שתי קבוצות מצבים $Q_1=F$, $Q_2=Q\setminus F$. עוד נגדיר $Q'=\{Q_1,Q_2\}$.

לולאות מקוננות: (3) ① נרוץ מ-$i=1$ עד שיתקיים תנאי העצירה (יפורט בהמשך), כך שבכל איטרציה i מקודם ב-1.

נעתיק את כל הקבוצות מצבים ב-Q' אל Q_i.

② נעבור בלולאה j על כל האותיות ב-$\sigma_j\in\Sigma$.

③ נעבור בלולאה k על כל קבוצות המצבים $Q_k\in Q_i$.

④ נעבור בלולאה על כל המצבים $q\in Q_k$.

נחשב $\delta(q,\sigma_j)$ ונסמן את q באינדקס l של קבוצת המצבים $Q_l\in Q_i$ שאליה הגענו בחישוב לה.* $\delta(q,\sigma_j)\in Q_l$

נחלק את Q_k לתתי קבוצות לפי הסימונים בכל $q\in Q_k$. שני מצבים באותה תת-קבוצה אם סומנו באותו אינדקס.

נעדכן את Q_i שיתאים לכל החלוקות הביניים בכל $Q_k\in Q_i$.

אם לאחר העדכון $Q_i=Q'$, כלומר לא חילקנו אף $Q_k\in Q_i$ בעבור ל-4. אחרת, נעדכן $Q'=Q_i$ ונקדם את i.

נבנה את A'. (4) Q' - נגדירו להיות ה-Q' האחרון שהתקבל בשלב (3).

קבוצת מצבים $Q_k\in Q'$ היא מצב ... ב-A'.

q_0' - נגדירו להיות קבוצת המצבים ב-Q' המכילה את q_0 של A.

F' - כל קבוצות המצבים $Q_k\in Q'$ המכיל מצב מקבל ב-A. $F'=\{Q_k\in Q':Q_k\cap F\neq\emptyset\}$.

δ' - נסמן לכל $Q_k\in Q'$ נציג $[q_k]$ כאשר $q_k\in Q_k$. נגדיר את פונקציית המצבים ב-A' כך:

כאשר קיימים $q_k\in Q_k$ ו- $q_l\in Q_l$ המקיימים $\delta(q_k,\sigma)=q_l$. $\delta'(Q_k,\sigma)=Q_l$, $\forall\sigma\in\Sigma$, $\forall Q_k\in Q'$

(5) נחזיר $A'=(Q',q_0',\Sigma,F',\delta')$.

הרעיון באלגוריתם Moore שהוא מחלק את Q_1 ו-Q_2, שהגדרנו בתחילת האלגוריתם, עד שהם מתאימים למחלקות השקילות של R_L, ולאחר מכן בונה את האוטומט A_L כמו בהוכחת הכיוון השני של נרוד. אלגוריתם זה רץ בזמן פולינומי בגודל הקלט. על אוטומט סופי דטרמיניסטי. לאוטומט סופי לא דטרמיניסטי אין אלגוריתם פולינומי כזה (אלא אם כן $P=NP$).

<u>הוכחת נכונות חלקית</u>

טענה: זוג מצבים $p,q\in Q$ יופרדו לקבוצות שונות ב-$\hat{Q}$ לראשונה בסוף האיטרציה ה-i אם ורק אם ה-z המפריד הקצר ביותר בין שני המצבים הוא באורך i. בפרט, אם ה-z המפריד הקטן ביותר בין כל שני מצבים באורך n, אזי האלגוריתם יעצור לכל היותר באיטרציה ה-$n+1$, שהרי לא יהיה בה שום שינוי.

לא רצה מ-$i=1$ נגדיר $i=0$ שלב תחול.

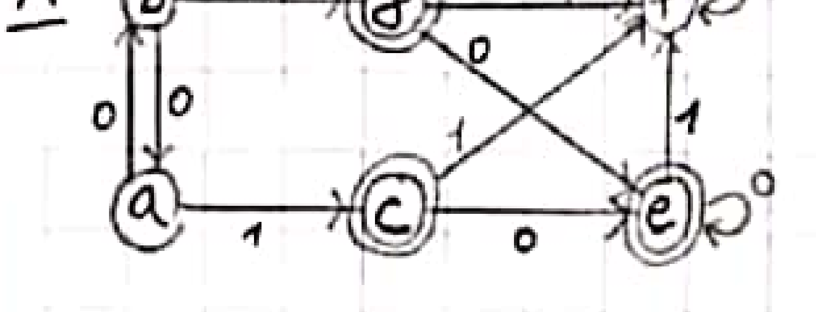
הוכחה: באינדוקציה על i.

בסיס - עבור $i=0$ יופרדו F ו-$Q\setminus F$, ואכן אלו בדיוק קבוצות המצבים שמפרידה ביניהם $z=\varepsilon$ מילה באורך 0 שהיא אכן המפריד הקצר ביותר ביניהם.

צעד - נניח את נכונות הטענה עבור i ונוכיח עבור $i+1$. נראה כל כיוון בנפרד.

כיוון 1: נניח שה-z המפריד הקצר ביותר בין p ל-q הוא באורך $i+1$. נראה ש-p ו-q יופרדו באיטרציה ה-$i+1$. נסמן $z=\sigma z'$ להיות המפריד הקצר ביותר. עוד נסמן $\delta(p,\sigma)=p'$ ו-$\delta(q,\sigma)=q'$. בלי הגבלת הכלליות, נניח כי $\delta(p',z')\in F$ אך $\delta(q',z')\notin F$, שהרי z מפריד מינימלי באורך $i+1$ ולכן z' הוא מפריד מינימלי באורך i. לכן לפי הנחת האינדוקציה p' ו-q' יופרדו באיטרציה ה-i. ומכאן שבאיטרציה ה-$i+1$, במעבר על σ, גם p ו-q יופרדו.

כיוון 2 - נניח ש-p ו-q הופרדו באיטרציה ה-$i+1$, נראה שה-z המינימלית המפרידה ביניהם גם היא באורך $i+1$. מהנחת הכיוון השני נובע כי באיטרציה ה-$i+1$ p ו-q הופרדו על ידי σ כלשהי המקיימת $\delta(p,\sigma)=p'$ ו-$\delta(q,\sigma)=q'$, כך ש-p' ו-q' בקבוצות שונות. נוכל להסיק מכך כי p' ו-q' הופרדו לראשונה באיטרציה ה-i, אחרת p ו-q היו נפרדים קודם, מהנחת האינדוקציה ישנו z' מפריד מינימלי באורך i בין p' ל-q'. נגדיר $z=\sigma z'$. נשים לב כי z מפרידה בין p ל-q וארוכה $i+1$. היא חייבת להיות מינימלית, כי אחרת p ו-q היו נפרדים קודם לפי הנחת האינדוקציה.



<u>דוגמא:</u> נריץ את האלגוריתם על האוטומט משמאל:

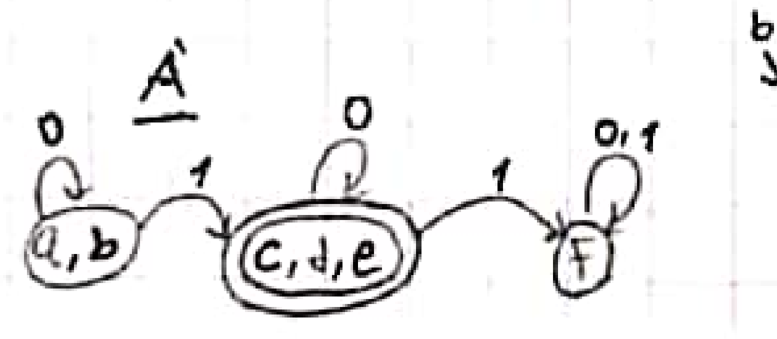
(1) סילוק מצבים לא עושה כלום. (2) אתחול: $Q_1=\{c,d,e\},\ Q_2=\{a,b,F\}$

$\sigma_j=0$: $\{a,b,F\}\{c,d,e\} \to b\ a\ F \mid e\ e\ e \to Q_1,\ Q_2$

$\sigma_j=1$: $\{a,b,F\}\{c,d,e\} \to c\ d\ F \mid F\ F\ F \to Q_2,\ Q_1,\ Q_1$

(3) איטרציה $i=1$: $\Rightarrow Q_1=\{a,b\},\ Q_2=\{c,d,e\},\ Q_3=\{F\}$

איטרציה $i=2$: אף נפריד Q_i לא ישתנה. עבור ל-4.



(4) נבנה את האוטומט A' לפי הציור משמאל ונחזיר אותו.

שיטה נוספת להרצה יעילה של שלב (3) של האלגוריתם, היא לבנות טבלה ריבועית, שבה כל שורה מייצגת מצב אחר ב-A. כל תא בטבלה (p,q) ננסה למצוא בו z מעביר בין q ל-p. אם מצאנו, נסמן את התא, אחרת נשאיר ריק.

חצי הטבלה שמתחת לאלכסון ראשי מיותר שכן התאים משוכפלים, לכן נסמן אותם ב-'. עבור קבוצות המצבים Q_1 ו-Q_2 שמוגדרות עם שלב האתחול באלגוריתם, ה-z המעביר בין המצבים משני הקבוצות הוא ε. בכל איטרציה נסרוק את כל התאים הריקים ונחפש אות מ-Σ שתעביר ביניהם. אם באיטרציה כלשהי לא היה שינוי בטבלה נעבור לשלב (4). נעבור שורה מלמעלה למטה, ובכל שורה של מצב p כל המצבים שהעמודות שלהם ריקים בשורה זו אומר שהם עם p באותה קבוצת מצבים ב-Q'. דוגמא להרצה כזו בסוף תרגול 4.