منابع :

1. https://www.eecs.yorku.ca/course_archive/2008-09/W/6115/palindrome.pdf

2. Hennie 1965 مقاله
https://doi.org/10.1016/S0019-9958(65)90399-2

3. Dexter C. Kozen, ToC,
The Complexity of Computation

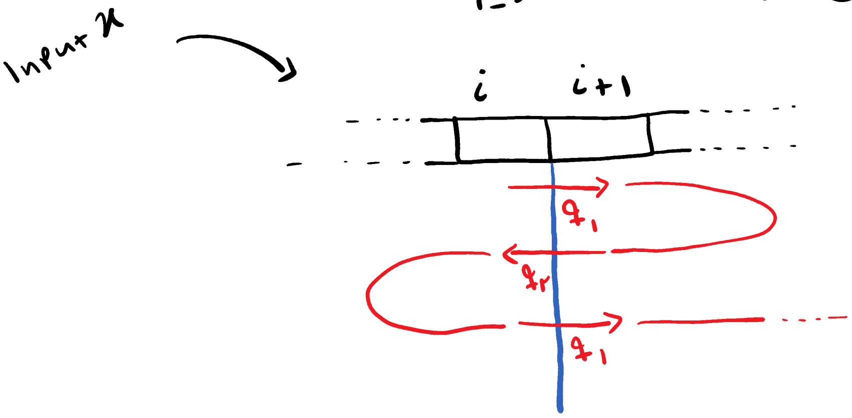
Thm. 1 : هر ماشین تک‌نواره‌ی تورینگ که PAL را decide می‌کند از مرتبه‌ی $\Omega(n^2)$ در worst-case مساله را حل می‌کند.

شهود : تکه‌های اطلاعاتی که TM باید آن‌ها را با هم مقایسه کند دور از هم افتاده اند. زمانی که هر از یک کاراکتر به کاراکتر متناظرش مانند $a_1 a_2 a_3 a_3 a_2 a_1$ حرکت می‌کند تنها می‌تواند مقدار ثابتی Information وابسته به تعداد هر state هایش حمل کند.

برای اثبات ابتدا می‌بایست Crossing sequence را تعریف کنیم.

تعریف Crossing sequence از کتاب زیر:
Formal Languages and Their relation to Automata (1969)
نوشته‌ی Hopcroft صفحه‌ی ۱۴۳ بخش ۱۰.۴ با عنوان Single-tape Turing machines And crossing sequences خواهد آمد.

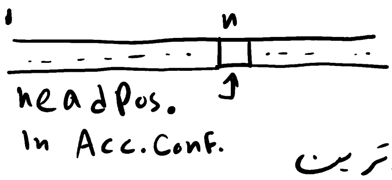
Crossing sequence : آن را با $C_i(x)$ نشان می‌دهند؛ دنباله‌ای از $q_x \in Q$ است هنگامی که از مرزبین خانه‌ی i و $i+1$ رد می‌شویم.



$$\Rightarrow C_i(x) = q_1, q_2, q_1$$

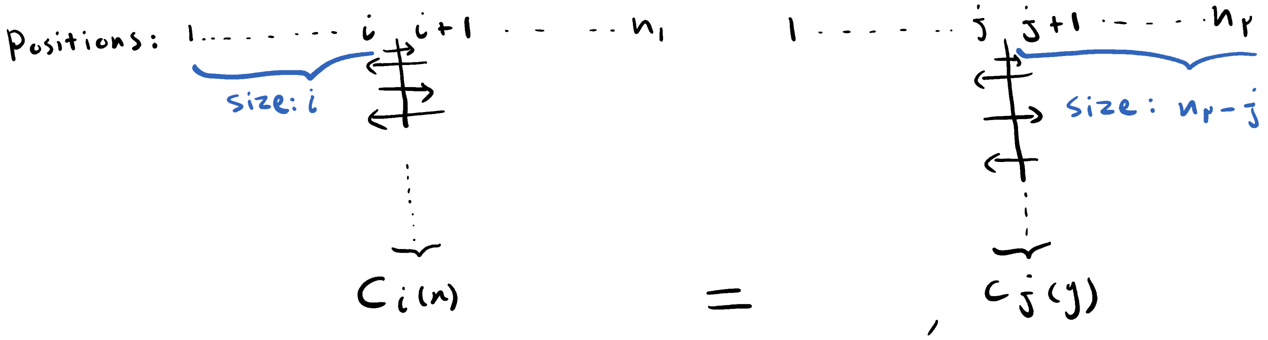
توجه شود که اولین عنصر هر $C_i(x)$ یک right crossing است و به همین ترتیب هر اندیس $2K-1$ از $C_i(x)$ یک right crossing است و هر اندیس $2K$ یک Left crossing است.

ما این جا فرض می‌کنیم ماشین در حالت accept لزوماً در پوزیشنی خواهد بود که دقیقاً در راستِ ورودیِ اصلی است:



این فرض مشکلی به وجود نمی‌آورد و ممکن است در بدترین حالت تعداد قدم‌ها را دو برابر کند. مثلاً فرض کنید M روی x، $T(x)$ قدم رفته است و در حال حاضر در سمت راست رشته‌ای تولید شده به اندازه‌ی $T(x)$ است، حال باید این مسیر را به عقب بازگردد که $T'(n) \leq 2T(n)$ را نشان می‌دهد. ولی این ضریب ۲ برای استفاده‌های ما مشکلی به وجود نمی‌آورد.

لم ۱ : اگر $x = a_1 a_2 \cdots a_{n_1}$ و $y = b_1 b_2 \cdots b_{n_2}$ توسط TM تکنواره‌ی M پذیرفته شود و $C_i(x) = C_j(y)$ به شکلی که $1 \le i < j$ آنگاه $z = a_1 a_2 \cdots a_i b_{j+1} \cdots b_{n_2}$ نیز توسط M پذیرفته خواهد شد :



$$z = \overbrace{a_1 \cdots a_i}^{x'} \overbrace{b_{j+1} \cdots b_{n_2}}^{y'}$$

$$C_i(x) = C_j(y)$$

$$\Downarrow$$

$$\boxed{x'y' \in L(M)}$$

Proof : ایده‌ی اثبات ما نه اثبات regular بودن زبان TM هایی است که روی Input Portion فقط خواندنی اند. [در آن جا روی CrossingSequence بین n و n+1 استقرا زدیم]

در این جا نیز به شکل جالبی از ایده‌ی بلاک بندی کردن execution استفاده شده است و event ها این جا crossing هاب شکل leftCrossing و RightCrossing می باشند.

می خواهیم اثبات کنیم اگر: $x = \underbrace{a_1 \cdots a_i}_{t_1} \underbrace{a_{i+1} \cdots a_{n_1}}_{t_2} \in L(M)$

$y = \underbrace{b_1 \cdots b_j}_{t_3} \underbrace{b_{j+1} \cdots b_{n_2}}_{t_4} \in L(M)$

آن‌گاه: $\underline{t_1 t_4 \in L(M)}$، اثبات با استقرا روی cross-event ها.

آن‌چه با استقرا ثابت می‌کنیم: Cross-event ها Computation را به چند بلاک افراز می‌کنند، اگر برای مثال $K = |C_i(x)|$ آن‌گاه داریم:

$$B_x^0 \xrightarrow{cross} B_x^1 \xrightarrow{cross} B_x^2 \cdots B_x^K$$

head position

$$\underbrace{(0, q_0, t_1 t_2)_x \vdash^* (i, q_x, \alpha a_i t_2)_x}_{B_x^0} \vdash^1 \overbrace{(i+1, q_y, \alpha a_i' t_2)_x \vdash^* (i+1, \ldots)_x}^{B_x^1}$$

right-crossing (event)

حال می خواهیم ثابت کنیم که اولین configuration هر بلاک $\underline{B_z^K}$ که $z = t_1 t_4$ است.

به شکل $(i+1, q_x, \underbrace{a_1 \cdots a_i}_{\alpha} \underbrace{a_{i+1} \cdots}_{\beta})_z$ اگر K فرد باشد و

$(i, q_x, \underbrace{a_1 \cdots a_i}_{\alpha} \underbrace{a_{i+1} \cdots}_{\beta})_z$ اگر K زوج باشد.

را اگر به شکل $\alpha = a_1 \cdots a_i$ و $\beta = a_{i+1} \cdots$ تجزیه کنیم آن‌گاه داریم

$(Pos, q_x, \alpha\beta)_z$ و $Pos = i + (K\%2)$ که در بلاک متناظر روی ورودی x و y به ترتیب داریم:

$(Pos, q_x, \underline{\alpha}\beta')_x$ و $(Pos, q_x, \alpha'\underline{\beta})_y$ یعنی i خانه‌ی ابتدایی اولین Conf. در $\underline{B_z^K}$ برابر $\underline{\alpha}$ و برابر i خانه‌ی ابتدایی اولین Conf. در $\underline{B_x^K}$ است. به همین ترتیب از خانه‌ی i+1 به بعد در اولین Conf بلاک $\underline{B_z^K}$ برابر $\underline{\beta}$ و برابر محتوای از خانه‌ی j+1 به بعد در اولین Conf بلاک $\underline{B_y^K}$ می‌باشد.

حال برای Basis اول $|C_i(n)|=1$ داریم:

InitConf: $q_0 t_1 t_2 = q_0\ a_1 a_2 \dots a_i b_{j+1} \dots b_{n_2}$

حال تا جایی که هدروی b_{j+1} قرار نگرفته است M رفتار مشابهی را با ورودی x دارد پس داریم:

on z:

$$\underbrace{(0, q_0, t_1 t_2)_z \vdash^* (i, q_y, \alpha_1 a_i t_2)_z}_{B^0_z} \overset{\text{Cross}}{\vdash} (i+1, q_x, \alpha_1 a'_{i_1} t_2)$$

و همینطور:

on x:

$$\underbrace{(0, q_0, t_1 t_2)_x \vdash^* (i, q_y, \alpha_2 a_i t_2)_x}_{B^0_x} \overset{\text{Cross}}{\vdash} (i+1, q_x, \alpha_2 a'_{i_2} t_2)$$

حال می‌دانیم که چون t_1 که TM آن را پردازش کرده همان n کاراکتر ابتدایی x هستند پس $\alpha_1=\alpha_2$ و روی یک state با نام q_y هم خواهیم بود: $(i, q_y, \alpha_1 a_i t_2)_z$، نتیجه‌ی $\delta_M(q_y, a_i)$ نیز یکی است پس نشان دادیم که $a'_{i_1} = a'_{i_2}$ همچنین می‌دانیم که اولین Conf. در بلاک B'_y برابر $(j+1, q_x, \alpha_3 t_2)_y$ است، چراکه بلافاصله بعد از Cross تنها t_3 در پردازش به α_3 تبدیل شده و هنوز هدروی t_2 قرار نگرفته است. حال n خانه‌ی ابتدایی در اولین Conf مربوط به اولین B'_z در conf. مربوط به اولین $\alpha'_1 a'_{i_1}$ هستند که $\alpha'_2 a'_{i_2} = \alpha'_1 a'_{i_1}$ و $\alpha'_2 a'_{i_2}$ مربوط به اولین Conf در B'_x هستند که برابرند. همچنین از خانه‌ی $i+1$ به بعد tape در اولین Conf، B'_z برابر از خانه‌ی $j+1$ به بعد در اولین Conf، B'_y است که همان t_2 است.

پس برای $i = 1$ Basis را اثبات کردیم.

حال برای یک مرحله جلوتر نیز آن را به عنوان Basis دوم اثبات می‌کنیم هرچند شاید ضروری نباشد. آن چه از $|C(x)|=1$ داشتیم:

$$\text{on } x: (0, q_0, t_1 t_2) \vdash^* (i+1, q_x, t_1' t_2) \vdash^* (i+1, q_y, t_1' t_2') \vdash (i, q_k, t_1' a' t_2'')$$

$$\text{on } y: (0, q_0, t_3 t_4) \vdash^* (j+1, q_x, t_3' t_4) \vdash^* (j+1, q_z, t_3' t_4') \vdash (j, q_k, t_3' b' t_4'')$$

$$\text{on } z: (0, q_0, t_1 t_4) \underset{\text{Cross}}{\vdash^*} \underbrace{(i+1, q_x, t_1' t_4) \vdash^* (i+1, q_z, t_1' t_4')}_{B_z^1} \underset{\text{Cross}}{\vdash} (i, q_k, t_1' b' t_4'')$$

اولین Conf. از B_z^1

اولین Conf از B_z^2

همانطور که در بالا مشاهده می‌شود از آن جا که سمت راست موقعیت i در اولین Conf. در B_z^1 برابر سمت راست موقعیت i در اولین Conf در B_y^1 است و در B_z^1 و B_y^1 هرگز از موقعیت فعلی چپ تر نمی‌رویم، پس سمت چپ موقعیت فعلی هم در این دو Conf در محاسبه‌ی این بلاک تأثیر ندارد و در انتهای بلاک، یک لحظه پیش از آن که از $i+1$ به i برویم، سمت راست موقعیت i و همچنین حالت فعلی در این دو یکسان خواهد بود. همچنین i خانه‌ی ابتدای نوار بی تغییر با آن چه در اولین Conf. B_z^1 بود یعنی t_1' باقی می‌ماند چون هنوز Cross اتفاق نیفتاده تا از $i+1$ چپ تر برویم. در Basis قبلی برابری i خانه‌ی ابتدای نوار را با همان t_1' را با i خانه‌ی ابتدایی در اولین Conf. بلاک B_x^1 را نشان دادیم به همین علت هر دو را t_1' نوشتیم.

یک لحظه پیش از رفتن به خانه‌ی $i+1$ به i، بعد در آخرین Conf بلاک B_z^2 روی اولین کاراکتر t_4' با نام b قرار دارد، حال کاراکتر $i+1$ در اولین Conf بلاک B_z^2 برابر $\delta_m(q_y,b)$ یا b' خواهد بود که با کاراکتر $i+1$ در اولین Conf بلاک B_y^2 برابر است حال از $i+1$ به بعد برابر $b' t_4''$ است و i خانه‌ی ابتدایی t_1' هستند.

حال که برای ۲ تا Basis یعنی: $|C_i(x)|=1$ و $|C_i(x)|=2$ اثبات شد، برای قدم استقرا فرض کنیم از B_z^K به B_z^{K+1} می‌رویم و K زوج است. فرض استقرا می‌گوید که برای B_z^K و B_x^K و B_y^K پیش از Cross داریم: $[2<K]$

$$\text{On } x: (i, q_x, \alpha_1\beta_1) \vdash^* (i, q_y, \alpha_1' a \beta_1) \vdash (i+1, q_z, \alpha_1' a' \beta_1)$$

$$\text{On } y: (j, q_x, \alpha_2\beta_2) \vdash^* (j, q_z, \alpha_2' b \beta_2) \vdash (j+1, q_z, \alpha_2' b' \beta_2)$$

$$\text{On } z: \underbrace{(i, q_x, \alpha_1\beta_2) \vdash^* (i, q_y, \alpha_1' a \beta_2)}_{\text{Induction Hypothesis} \rightsquigarrow B_z^K} \underbrace{\vdash}_{\text{Cross}} \underbrace{(i+1, q_z, \alpha_1' a' \beta_2)}_{B_z^{K+1}}$$

در B_z^K براساس فرض استقرا برابری i کاراکتر اول نوار بین اولین Conf در B_z^K و اولین Conf در B_x^K برقرار است. همچنین طبق فرض استقرا برابری محتوای tape از $i+1$ به بعد در اولین Conf بلاک B_z^K و محتوای tape از $i+1$ به بعد در اولین conf بلاک B_x^K برقرار است. حال از آن جا که K زوج است، از i در محاسبه‌ی B_z^K سمت راست‌تر نخواهیم رفت و به همین ترتیب از i راست‌تر در محاسبه‌ی B_x^K نخواهیم رفت. از آن جا که بخش تاثیرگذار اولین Conf این دو بلاک $[B_z^K$ و $B_x^K]$ برابر بوده و هد روی بخش غیرمشترکشان نخواهد رفت پس i کاراکتر اول در آخرین conf B_z^K برابر با i کاراکتر اول در آخرین Conf بلاک B_x^K خواهد بود. یک لحظه پیش از رویداد، یعنی قبل از رفتن از i به $i+1$ (cross) در آخرین Conf بلاک B_z^K هستیم و هد روی کاراکتر iام است. پس کاراکتر iام در اولین Conf بلاک B_z^{K+1} برابر $\delta_M(q_y, a)$ است که a کاراکتر iام در آخرین Conf بلاک B_z^K است. این مقدار برابر با iامین کاراکتر در اولین Conf در B_x^{K+1} چرا که این دو رفتار مشابه داشتند. [ص بعد]

همچنین دقت شود که حالت فعلی در آخرین conf در بلاک B_z^K نیز برابر با حالت فعلی در آخرین conf در بلاک B_x^K چراکه بخش تاثیرگذار در محاسبه‌ی بلاک B_z^K و B_x^K در اولین conf این بلاک ها مشترک بوده است، نام این حالت را q_y می گذاریم. حال اگر $\delta_m(q_y,a)=a'$ آن گاه نا کارکتر ابتدایی B_z^{K+1} برابر $\alpha a'$ و برابر نا کارکتر اول B_x^{K+1} خواهد بود.

حال توجه شود که بخش غیر تاثیرگذار در B_z^K، از آنجا که در بلاک زوج هستیم دست نخورده باقی می ماند و به B_z^{K+1} منتقل می شود. نام این بخش را یعنی محتوای خانه‌های حافظه از $i+1$ به بعد را β_2 نام گذاری کردیم، این بخش در B_z^K و B_z^{K+1} مشترک است و بر اساس فرض استقرا برابر است با محتوای نوار از خانه‌ی $j+1$ به بعد در اولین conf بلاک B_y^K. در این جا نیز، از آن جا که K زوج است، β_2 در محاسبه‌ی B_y^K تاثیرگذار نیست و دست نخورده به B_y^{K+1} منتقل می شود. پس β_2 برابر با محتوای نوار از خانه‌ی $j+1$ به بعد در B_y^{K+1} است.

به این ترتیب برای K زوج قضیه را اثبات کردیم.

حال فرض کنیم K فرد است و قضیه برای B_z^K و B_y^K و B_x^K برقرار است، حال داریم:

$$\text{On } x: (i+1, q_x, \alpha_1\beta_1) \vdash^* (i+1, q_y, \alpha_1 a \beta_1') \overset{\text{cross}}{\vdash} (i, q_K, \alpha_1 a' \beta_1')$$

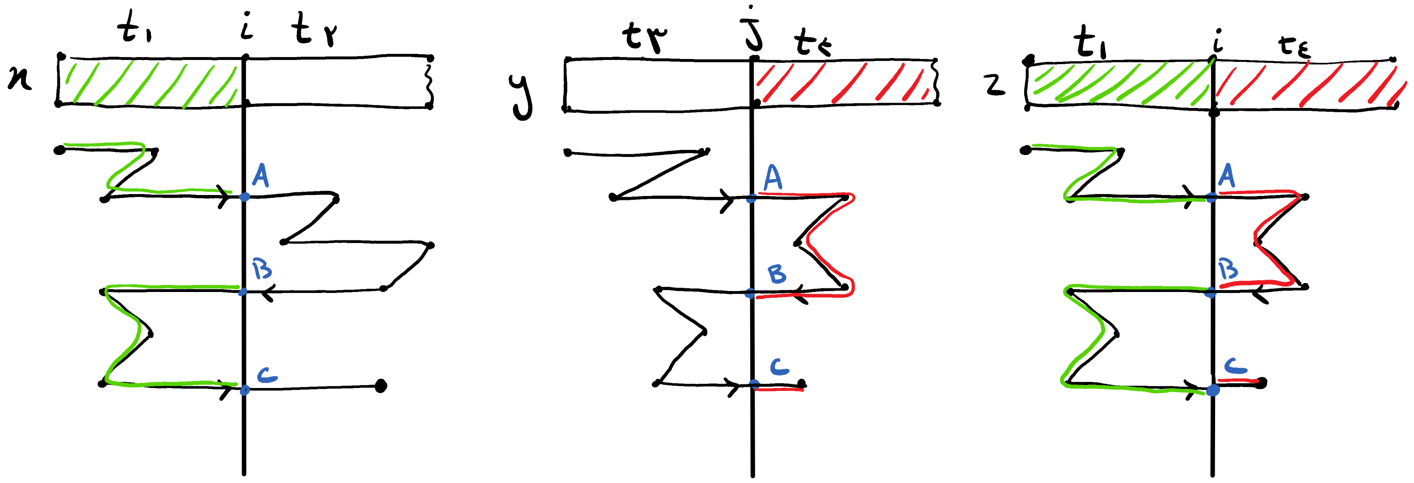
$$\text{On } y: (j+1, q_x, \alpha_2\beta_2) \vdash^* (j+1, q_z, \alpha_2 b \beta_2') \vdash (j, q_K, \alpha_2 b' \beta_2')$$

$$\text{On } z: (i+1, q_x, \alpha_1\beta_2) \vdash^* (i+1, q_z, \alpha_1 b \beta_2') \vdash (i, q_K, \alpha_1 b' \beta_2')$$

اثبات مشابه است. بخش بی تاثیر در این جا به تقارن بخش قبل، نا کارکتر ابتدایی نوار می باشند. به همین علت این بخش دست نخورده به بلاک بعدی منتقل می شود. بخش تاثیرگذار در محاسبه‌ی بلاک نیز به علت فرض استقرا در بلاک K و ورودی y برابر است با همان بلاک z و به همین ترتیب اثبات می شود.

توجه شود که علت یکی گذاشتن حالت فعلی در اولین conf هر بلاک در x، y و z برابر بودن $C_j(y) = C_i(x)$ است که در اثبات به صورت ضمنی از آن استفاده کردیم.

حال با اثبات این قضیه می‌توانیم به راحتی استدلال کنیم که اگر $x = t_1 t_2$ و i ، t_1 کارکتر ابتدای x و $y = t_3 t_4$ که j ، t_3 کارکتر ابتدایی y است و $x, y \in L(M)$ و $C_i(x) = C_j(y)$ آن‌گاه $z = t_1 t_4 \in L(M)$ ، ابتدا شمای این اتفاق را مطابق با مقاله‌ی Hennie در 1965 می‌کشیم:

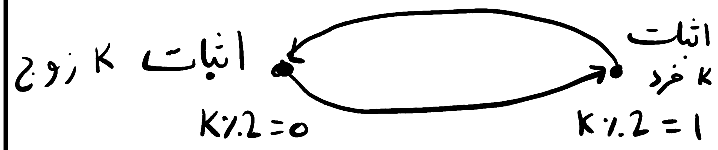


در شکل بالا $C_i(x) = C_j(y) = [A, B, C]$ حال می‌خواهیم نشان دهیم اگر $x, y \in L(M)$ آن‌گاه $x' = t_1$ و $y' = t_4$ پس $z = x'y' \in L(M)$. لم ۱

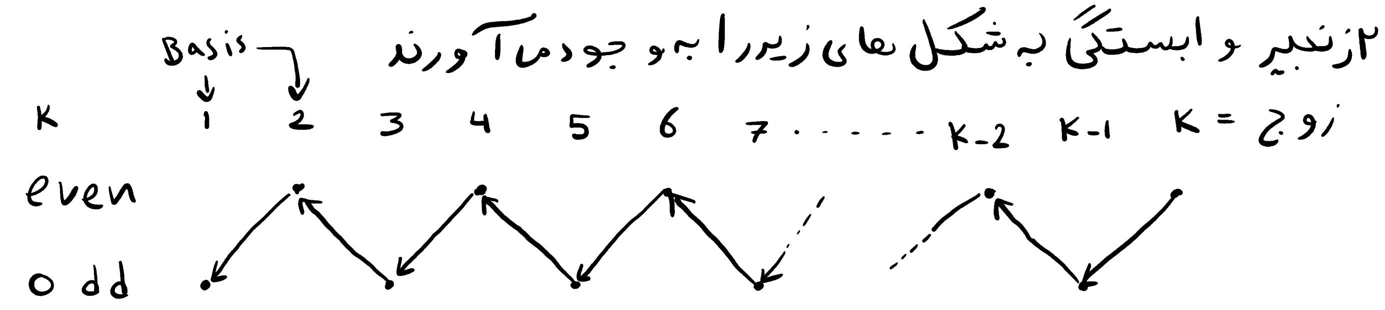
Proof: اگر $C_j(x) = C_i(x)$ پس اندازه‌ی آن‌ها نیز برابر است در نتیجه B_x^K در x پذیرفته می‌شود و y در B_y^K ، حال اگر K زوج باشد آن‌گاه Halt و Accept در i خانه‌ی ابتدایی نوار اتفاق خواهد افتاد. از آن‌جا که در K های زوج از i+1 خانه به بعد نوار بی‌تاثیر در محاسبه هستند پس در بلاک متناظر B_z^K نیز به علت برابر بودن محاسبه‌ی آن با B_x^K رشته پذیرفته خواهد شد، همین استدلال بدون از دست دادن عمومیت [w.l.o.g] برای K فرد برقرار است. ∎

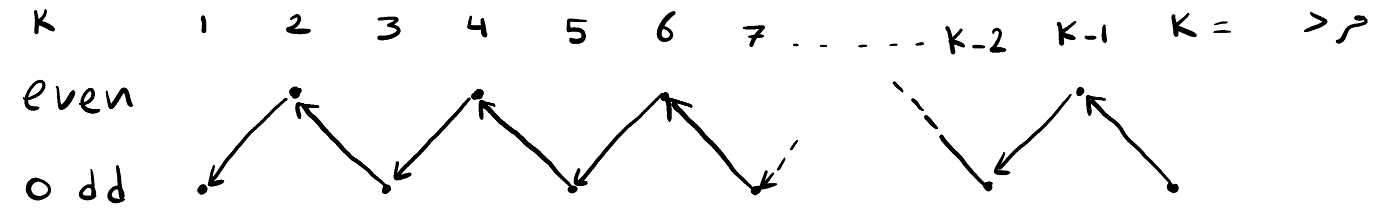
پیش از ادامه یک نکته را در مورد قضیه‌ی برابری بلاک‌ها روشن می‌کنیم.

قدم استقرا در اثبات این قضیه به این شکل بود که برای K+1 فرد با فرض درست بودن K زوج اثبات می‌شد و برای K+1 زوج با فرض درست بودن K فرد اثبات شد. ممکن است این تصور اشتباه صورت گیرد که اثبات ما به شکل یک سیکل است و در نتیجه اشتباه است یعنی:



ولی این طور نیست، برای K دلخواه این K یا زوج است یا فرد، اگر زوج باشد اثبات به درستی K قبلی اش که فرد است وابسته است و اگر فرد باشد اثبات به درستی K قبلی اش که زوج است وابسته است. در یک مرحله بیشتر پیش رفتن دوباره درستی زوج قبلی به فرد قبلی اش و به همین قرینه فرد قبلی به زوج قبلی اش وابسته است. گراف وابستگی این اثبات لزوماً DAG بوده و به Basis می‌رسد. ۲ حالت مختلف K = زوج و K = فرد ۲ زنجیر وابستگی به شکل های زیر را به وجود می‌آورند





همچنین در گراف وابستگی ص قبل دیده می‌شود که نیازی به اثبات ۲ تا Basis نبود و اثبات برای Basis با مقدار K=1 کافی بود.

چند نکته: اثبات قضیه‌ی برابری بلاک‌ها در هیچ کدام از منابع ① و ② نیامده بود. به طور خاص در ① به نحوه‌ی اثبات اشاره شده و آن چه ما به آن در این جا بلاک می‌گفتیم در آن جا با عنوان chunk معرفی شده و استقرا زده نشده ولی به این اشاره شده که استقرای اثبات این قضیه روی K است و تودرتو (nested) است (؟).
همچنین در مقاله‌ی اصلی 1965، یعنی منبع ②، پس از ارائه‌ی شهود از درستی این قضیه، درستی آن با عبارت "Almost intuitively obvious" بدون اثبات رها شده و تاکید شده که در این جا برای این قضیه "rigorous Proof" آورده نمی‌شود.
از این رو من با استفاده از Hint های منبع ① و شهود منبع ② اثبات این قضیه را اینجا انجام دادم.

یک نتیجه‌ی کاربردی از این قضیه: اگر $x = t_1 t_2 t_3$ باشد و Crossing Sequence مرز بین $t_1 t_2$ برابر Crossing Sequence مرز بین $t_2 t_3$ باشد آن‌گاه:

۱. رفتار ماشین M روی $t_1 t_3$ برابر $t_1 t_2 t_3$ خواهد بود.
۲. رفتار ماشین M روی $t_1 t_2 t_2 t_3$ برابر با $t_1 t_2 t_3$ خواهد بود.

[از آن جا که این نتایج و کاربرد آن‌ها در این جا به کار نمی‌آید، در حد اشاره به صورت آن‌ها کافیست برای اثبات مقاله‌ی Hennie، منبع ②]

حال می‌خواهیم Thm.1 یعنی $PAL \in \Omega(n^2)$ در TM تک‌نواره را اثبات کنیم.

ساختمان اصلی این اثبات منبع (۳)، یعنی لکچرنوت اول Dexter C. Kozen در درس ToC است. با این حال اندازه‌ی set زیرمجموعه‌ی PAL در این منبع مقدار کسری دارد. پس همین استدلال را روی set زیبای منبع (۱) می‌آوریم.

(۱) فرض می‌کنیم محاسبه در سمت راست‌ترین بخش nonblank در حالت Accept متوقف می‌شود. این فرض اشکالی ایجاد نمی‌کند چرا که به گفته‌ی Hopcraft در ضریب ۲ یا به گفته‌ی Kozen در ضریب ۴ تفاوت ایجاد می‌کند. [البته فرض Hopcraft کمی متفاوت است]

حال PAL_n را مانند منبع (۱) تعریف می‌کنیم: $PAL_n := \{w c^{2n} w^R \mid w \in \{0,1\}^n\}$

Note: روشن است که $PAL_n \subsetneq PAL$

حال $C(x)$ را مجموعه‌ی crossing sequence های از $n+1$ تا $3n$ تعریف می‌کنیم:

$$C(x) := \{C_i(x) \mid n+1 \le i \le 3n\}$$

حال در لم ۲ ثابت می‌کنیم که برای هر x و y، هیچ $C_i(x)$ و $C_i(y)$ در $C(x)$ و $C(y)$ پیدا نمی‌شود که برابر باشد، چرا که در آن صورت با استفاده از لم (۱) باید $z = x'y'$ هم در PAL باشد که در ادامه می‌بینیم این طور نخواهد بود:

لم ۲: برای هر $x, y \in PAL_n$ که $x \neq y$، $C(x) \cap C(y) = \emptyset$

Proof: فرض کنیم این طور نباشد و $c \in C(x) \cap C(y)$ آن‌گاه i و j وجود دارند در بازه‌ی $n+1 \le i, j \le 3n$ که $C_i(x) = C_j(x)$، آن‌گاه بر اساس لم (۱) اگر x'، i کاراکتر اول x و y'، از $j+1$ به بعد رشته‌ی y باشد، داریم: $z = x'y' \in PAL_n$

ولی z به شکل $x'y'$ نمی‌تواند پالیندروم باشد. چرا که $i \geq n+1$ پس x' شامل w و حداقل یک c است و از آن جا که $j \geq n+1$ پس حتما شامل صفر یا چند c و به دنبال آن یک w^R دیگر است. از آن جا که $x \neq y$ پس w^R در y' نمی‌تواند rev(w) باشد، در نتیجه داریم:

$w_1 c^K w_2^R$ که $w_1 \neq w_2$. روشن است که $w_1 c^K w_2^R \notin PAL$ در نتیجه

$w_1 c^K w_2^R \notin PAL_n$، که این تناقض است. پس $C(x) \cap C(y) = \emptyset$

■

ادامه‌ی اثبات Thm. 1 : m_x را کوچکترین $C_i(x)$ در $C(x)$ می‌گیریم:

$$m_x := \min\{|C_i(x)| \mid n+1 \leq i \leq 3n\}$$

ابتدا نشان می‌دهیم دست کم یک m_x وجود دارد که $m_x \geq n$، سپس چون m_x در بین همه‌ی crossing sequence های یک $x \in PAL_n$ با $i \in \{n+1, \dots, 3n\}$ است پس بقیه‌ی $C_i(x)$ ها نیز از $\Omega(n)$ هستند و در نتیجه $n^2 \leq \sum_{i=n+1}^{3n} C_i(x)$ و از آن جا که به ازای هر cross یک قدم در TM رفته‌ایم، وجود خواهد داشت x که روی TM تک‌نواره دست کم به $\Omega(n^2)$ زمان نیاز دارد.

ابتدا L را Max، m_x ها تعریف می‌کنیم: $L := \max\{m_x \mid x \in PAL_n\}$

تمام crossing sequence های ممکن به طول حداکثر L برابر $\sum_{i=0}^{L} |Q|^i = \frac{|Q|^{L+1}-1}{|Q|-1} = \alpha$

می‌باشد چرا که تعداد crossing sequence های ممکن به طول i برابر $|Q|^i$ است.

براساس لم ۲، هیچ ۲ رشته‌ای در PAL_n نمی‌توانند crossing sequence مشترکی در محدوده‌ی $n+1$ تا $3n$ داشته باشد. همچنین $|PAL_n| = 2^n$ پس *$\boxed{\alpha \geq 2^n}$* برقرار است.

$\alpha \geq 2^n$ چرا که تمام shortest crossing sequence های ممکن هر کدام یک crossing sequence

در بازه‌ی $n+1 \leq i \leq 3n$ هستند پس:

$$SCS := \{C_i(n) \mid C_i(n) = \text{Shortest Crossing Sequence in } i \in \{n+1 \dots 3n\}\}$$

$$SCS \subseteq \{\text{All Possible Crossing Sequence of length at most } L\}$$

البته پیش فرض $n \in PAL_n$ را نیز در نظر داریم. حال اگر $|SCS| < 2^n$ باشد یعنی i و j

در بازه‌ی $n+1 \leq j, i \leq 3n$ بر اساس Pigeonhole وجود دارند که $C_i(n) = C_j(y)$ و

$n \neq y$ که این تناقض با لم ۲ است. پس $\alpha \geq 2^n$ و همچنین

$$\alpha = \frac{|Q|^{L+1}-1}{|Q|-1} \rightsquigarrow |Q|^{L+1} \geq \frac{|Q|^{L+1}-1}{|Q|-1} \geq 2^n \rightsquigarrow |Q|^{L+1} \geq 2^n$$

$$\xrightarrow{\lg_{|Q|}} L+1 \geq \lg_{|Q|} 2^n \rightsquigarrow L+1 \geq n \underbrace{\lg_{|Q|} 2}_{\text{Constant}} \rightsquigarrow L+1 \geq \underset{\text{constant}}{c}\, n$$

$$\rightsquigarrow \boxed{L \in \Omega(n)}\ *$$

یادمان هست که L، maximum در بین m_n ها بود. یعنی $\exists n[m_n = L]$

از آن جا که $m_n = \min\{|C_i(n)| \mid n+1 \leq i \leq 3n\}$ پس:

$$\exists n\ \forall C_i(n)\ [n+1 \leq i \leq 3n \Rightarrow |C_i(n)| \geq L]$$

یعنی $2n$ مرز بین خانه‌ی $n+1$ و $3n$ وجود دارد که هر یک Crossing Sequence با اندازه‌ی

دست کم n دارند. از آن جا که For every $n \in PAL_n \rightsquigarrow T(4n) \geq \sum_{i=1}^{4n} |C_i(n)|$ و بر اساس بالا

داریم $\sum_{i=n+1}^{3n} |C_i(n)| \geq n^2$ پس $T(4n) \geq n^2$، در نهایت: $\boxed{T(n) \in \Omega(n^2)}$