

به نام خدا

نظریه زبان ها و ماشین ها- بهار ۱۴۰۳

پاسخنامه تمرین شماره 8

دستیار آموزشی این مجموعه: کسرا نوربخش

noorbakhshkasra04@gmail.com

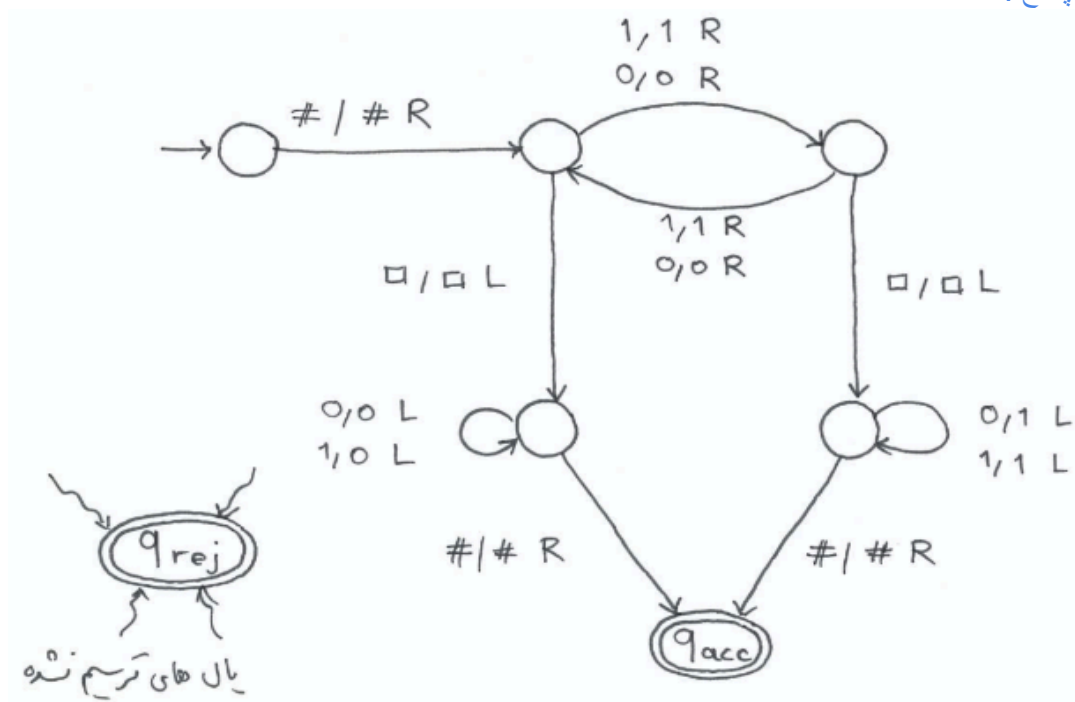
تاریخ تحویل: ۳۰ اردیبهشت (صفحه درس)

1. ماشین تورینگ متناظر هر بخش را طراحی کنید. (منظور ماشین تورینگ به همراه state diagram و تمامی جزئیات مربوط به جابجایی head میباشد) (۴۰ نمره)

- الف) ماشینی که روی ورودی w که در آن $w \in \{0,1\}^*$ ، موارد زیر را انجام دهد: $(w = |n|)$
- اگر n زوج باشد ورودی w را به 0^n تبدیل کند.
 - اگر n فرد باشد ورودی w را به 1^n تبدیل کند.

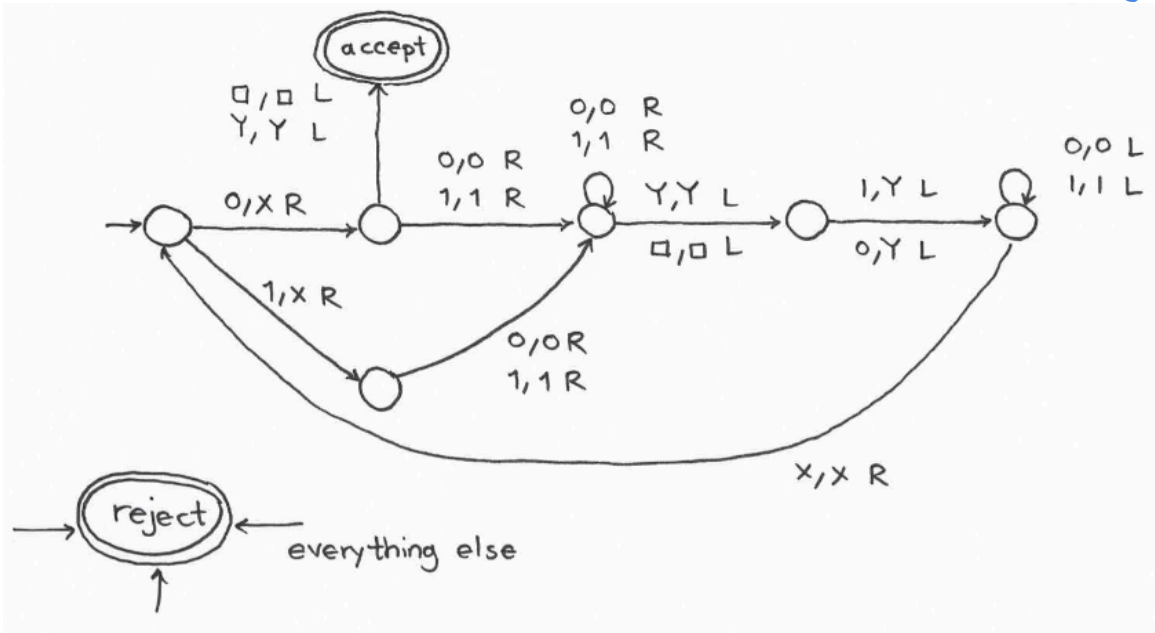
ماشین تورینگ پس از انجام تبدیل به حالت accept می رود. اگر ورودی به فرمت صحیح نباشد، باید آن را رد کند.

پاسخ:



ب) ماشینی که رشته هایی با طول فرد را بپذیرد که در آنها علامت میان رشته 0 است. به عنوان مثال 11001 و 1110111 پذیرفته می شوند اما 0000 و 110 پذیرفته نمی شوند. ($\Sigma = \{0,1\}$)

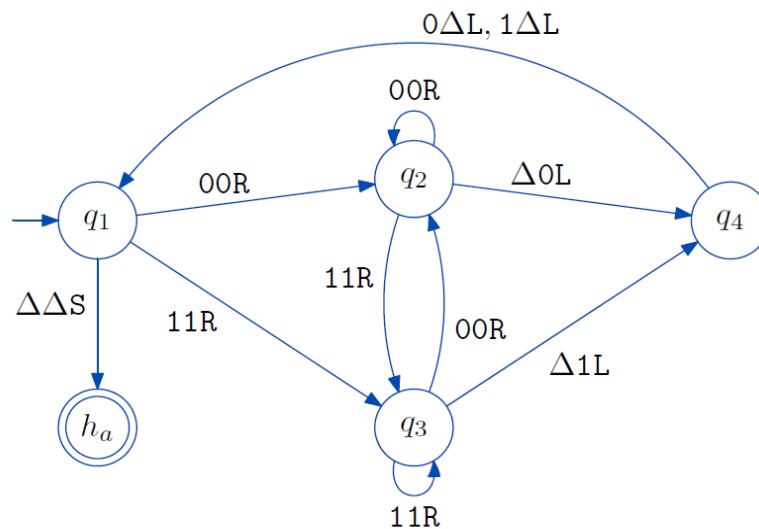
پاسخ:



ج) ماشینی که ورودی خود را (یک رشته باینری) ۱ واحد به سمت راست shift دهد. ($\Sigma = \{0,1\}$)

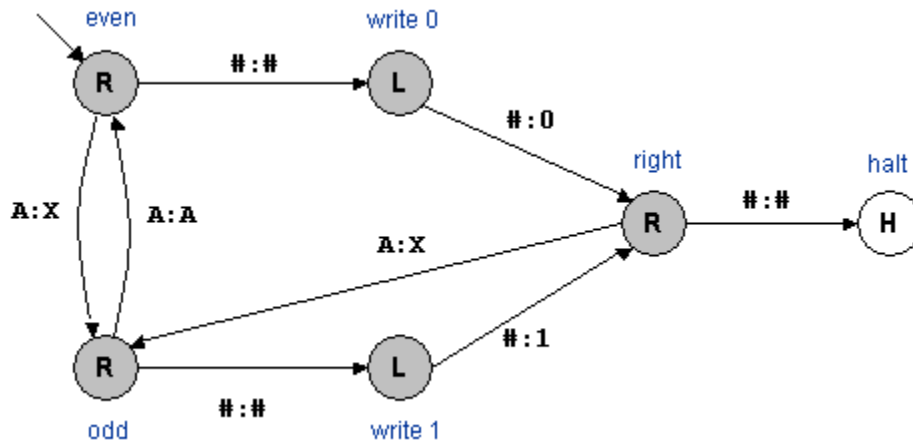
پاسخ:

TM for Shifting Right



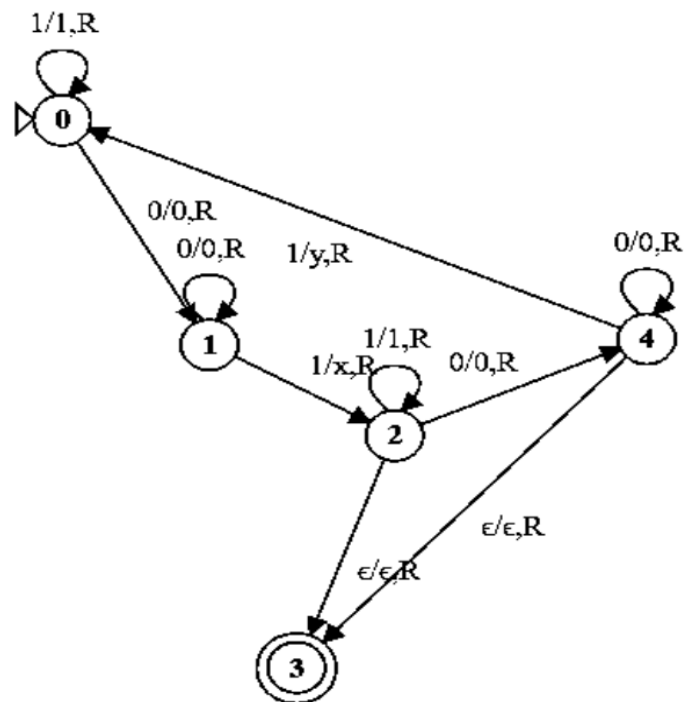
د) ماشینی که ورودی خود را (یک عدد به فرم unary) به binary تبدیل کند. ($\Sigma = \{0,1\}$)

to represent a number N in Unary, a symbol representing 1 is repeated N times.



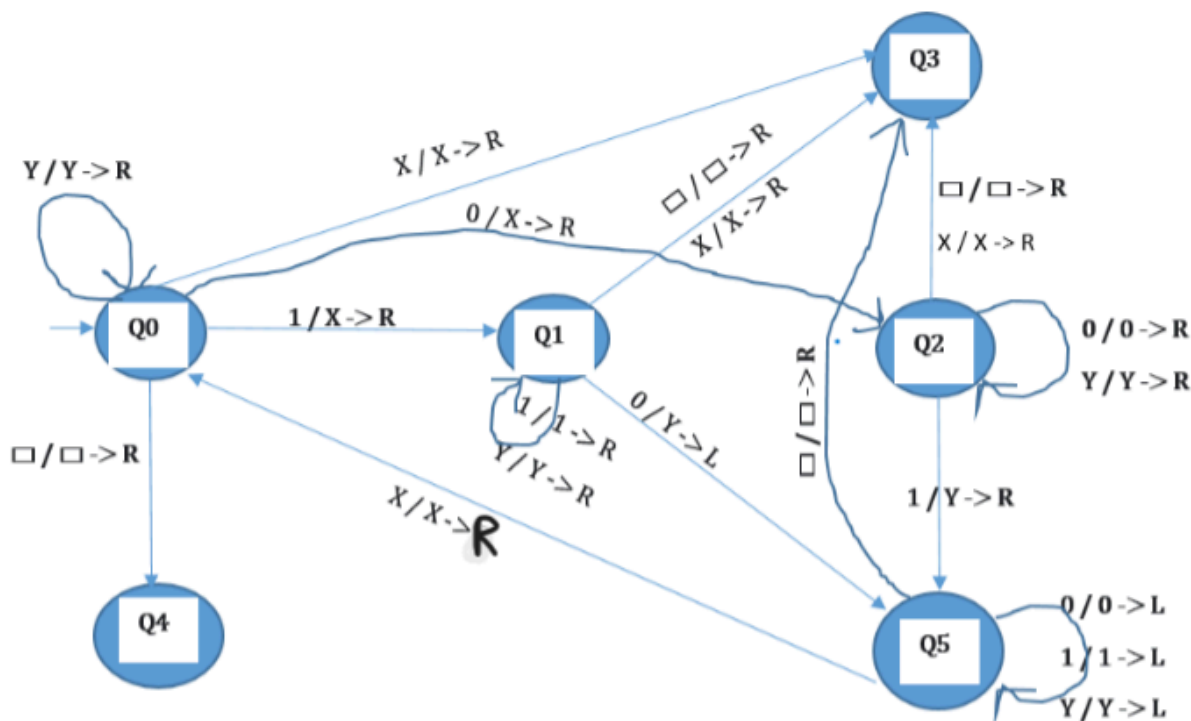
2. مشخص کنید هر کدام از ماشین تورینگ های زیر، چه زبانی را می پذیرند. (۲۰ نمره)

(الف)



پاسخ : این ماشین رشته هایی را توصیف میکند که به تعداد فرد تا '01' در آن ها داریم.

(ب)



پاسخ: این ماشین رشته‌هایی را توصیف می‌کند که تعداد ۰ها و ۱های رشته با همدیگر برابرند اما آخر رشته به ۱ ختم نمی‌شود.

3. برای زبان‌های زیر، یک ماشین تورینگ طراحی کنید. ارائه توصیف سطح بالا کفایت می‌کند. (۲۰ نمره)

الف) زبانی متشکل از رشته‌هایی بر روی الفبای $\{0,1\}$ که توسط \$ از یکدیگر جدا شده‌اند و هر دو رشته با یکدیگر تفاوت دارند.

پاسخ: ماشین تورینگ این سوال این گونه کار می‌کند که ابتدا رشته اول را با مابقی رشته‌ها مقایسه می‌کند اگر با تمامی آن‌ها فرق داشت رشته بعدی را به تمامی رشته‌های از آن به بعد مقایسه می‌کند و ...

الگوریتم آن:

۱- بر روی ورودی w بر روی چپ‌ترین سمبل علامت می‌گذاریم اگر بعدی blank بود می‌پذیریم اگر \$ بود به مرحله بعد می‌رویم در غیر این صورت reject می‌کنیم.

۲- تا \$ بعدی جلو می‌رویم و یک علامت بر روی آن می‌گذاریم اگر \$ دیگری قبل از به blank رسیدن ندیدیم پس فقط یک رشته داشتیم و می‌پذیریم.

۳- دو رشته‌ای که بعد از دو \$ علامت خورده قرار دارند را به صورت زیگ‌زاگی مقایسه می‌کنیم اگر یکی بودند reject می‌کنیم.

۴- راست‌ترین \$ علامت خورده را به \$ سمت راستی می‌بریم. اگر هیچ \$ ای قبل از رسیدن به blank نبود به چپ‌ترین \$ علامت خورده می‌رویم و آن را به \$ بعدی می‌بریم و راست‌ترین \$ علامت خورده را به بعدیش. اگر هیچ \$ ای در سمت راست سمت راست‌ترین \$ علامت خورده نبود پس تمامی رشته‌ها چک شده‌اند پی

می پذیریم.

ب) یک رشته از کاراکترهای a, b را در نظر بگیرید که طول رشته مضربی از عدد 3 است. این رشته را به سه قسمت مساوی تقسیم می کنیم. حال ماشین تورینگ طراحی کنید که قسمت میانی (قسمت دوم) از این رشته را معکوس کند و روی نوار قرار دهد. به عنوان مثال، رشته داده شده برابر است با: $abbabbaba$ با انجام این عملیات باید رشته bba رو نوار چاپ شود.

پاسخ: ابتدا باید یک سوم میانی این رشته را بیابیم. برای این کار به ازای هر یک کاراکتر که از ابتدا رشته می خوانیم دو کاراکتر از انتهای رشته می خوانیم. می توانیم هر کاراکتر را که می خوانیم به حرف بزرگش تغییر دهیم. به این ترتیب ابتدای این یک سوم را پیدا خواهیم کرد. برای به دست آوردن انتهای این یک سوم میانی هم می توانیم برعکس این عملیات را انجام دهیم یعنی دو کاراکتر از ابتدا و یک کاراکتر از انتهای آن بخوانیم. حال که ابتدا و انتهای این یک سوم را پیدا کردیم کافی است معکوس آن را در انتهای رشته چاپ کنیم. برای این کار از انتهای یک سوم شروع می کنیم و در انتهای رشته چاپ می کنیم.

4. در این سوال همان طور که هنگام حل مشاهده کردید، یک ماشین تورینگ بسیار بزرگ و پر استتیت جواب ما خواهد بود که ریز توصیف آن را می توانید از [این لینک](#) مطالعه بفرمایید.

5. توصیف سطح بالا از ماشین تورینگ که زبان زیر را می پذیرد بدهید. $(\Sigma = \{k, -, 1, 0\})$

(۱۰ نمره)

$L = \{w-k^n \mid w \in \{0, 1\}^*\}$ نمایش باینری عدد n است

مثال: $00011-kkk \in L$ and $001-kkk \notin L$

پاسخ: ماشین تورینگ این سوال این گونه کار می کند که از هر طرف - یکی یکی کم می کند تا یک طرف به ۰ برسد. اگر هر دو طرف همزمان به ۰ برسند پس برابر بوده اند و می پذیریم.

الگوریتم آن:

۱- بر روی ورودی اگر به فرم یک رشته و سپس یک - و تعدادی k نبود $reject$ می کنیم.

۲- اگر تعدادی ۰ قبل از - داشتیم و بعد از آن هیچ k ای نبود می پذیریم.

۳- سمت راست ترین k را به $blank$ تبدیل می کنیم. اگر k ای نبود $reject$ می کنیم.

۴- ۱ واحد از عدد باینری سمت چپ - کم می کنیم.

۵- به سمت چپ از - حرکت کرده و هر ۰ را به ۱ تبدیل می کنیم تا به ۱ برسیم. آن ۱ را ۰ می کنیم.

۶- اگر هیچ ۱ ای یافت نشد $reject$ می کنیم.

۷- به مرحله ۲ می رویم.

6. یکی از حالت های شکاندن یک الگوریتم رمزنگاری (encryption)، حالت آگاه بودن از متن رمز نشده است. در این حالت، یک متن رمز نشده که جاسوس آلمانی، کوروش برای ما آورده را به همراه نتیجه رمز شده آن در اختیار داریم و تنها به دنبال یافتن کلید رمزنگاری هستیم تا بتوانیم هیتلر را شکست دهیم و پیام های سری آن ها را رمزگشایی کنیم. حال یک الگوریتم رمزنگاری را تصور کنید که از الگوریتم آن آگاه نیستید اما یک ماژول رمزنگار (که همان Enigma می باشد) از این الگوریتم که توسط ماشین تورینگ پیاده سازی شده، به شما داده شده است. این ماژول یک متن رمز نشده به همراه یک کلید 8 بیتی را دریافت کرده و پس از پایان عملیات، متن رمز شده را به شما می دهد (در این مسئله می توانید فرض کنید نتیجه این ماژول در انتهای نوار ماشین تورینگ شما قرار می گیرد). حال، به شما یک متن رمز نشده به همراه نتیجه رمز شده آن داده شده و از شما خواسته شده که کلیدی که به وسیله آن، این متن را رمز کرده اند، بیابید و ادعا کنید که به اندازه آقای تورینگ باهوش هستید. تضمین می شود مسئله پاسخ دارد. یک توصیف سطح بالا از ماشین تورینگ که بتواند این کار را برای شما انجام دهد، ارائه دهید و نحوه قرار گرفتن ورودی روی نوار را نیز توضیح دهید. (امتیازی ۱۰ نمره) (شاید دیدن فیلم The Imitation Game برای حل این سوال راهگشا باشد!)

پاسخ:

فرض میکنیم ابتدا یک علامت \$ و سپس متن رمز نشده روی نوار قرار گرفته است. سپس، یک علامت \$ روی نوار قرار گرفته و پس از آن، متن رمز شده قرار گرفته است. در نهایت پس از یک علامت \$ یک عدد باینری 8 بیتی با مقدار اولیه 0 روی نوار قرار میگیرد.

- تا زمانی که از حلقه خارج شویم:

- کلید قرار گرفته را به همراه متن رمز نشده به ماژول رمزنگار میدهیم.

- نتیجه ماژول رمزنگار (انتهای نوار) را با متن رمز شده (بخش دوم) مقایسه میکنیم. این کار را میتوانیم با مقایسه و علامت زدن خانه به خانه این دو بخش انجام دهیم.

- اگر دو بخش برابر بودند، از حلقه خارج میشویم. در غیر اینصورت، نتیجه ماژول رمزنگار را از انتهای نوار حذف کرده و متن رمز شده را به حالت اولیه برمی گردانیم.

- به بخش کلید 8 بیتی رفته و مقدار آن را 1 واحد افزایش میدهیم. لازم به ذکر است که در این بخش نیازی به شیفت دادن رمز نیست زیرا مطمئنیم کلید 8 بیتی است و از همان ابتدا 8 بیت برای آن در نظر گرفته ایم.

به این کار، Brute Force گفته میشود.

We can only see a short distance ahead, but we can see plenty there that needs to be done.

Alan Turing

