دانشگاه تهران
پردیس دانشکده‌های فنی
دانشکدهٔ مهندسی برق و کامپیوتر

روش‌های رسمی در مهندسی نرم‌افزار

تمرین کامپیوتری Spin

هادی صفری
hadi.safari@ut.ac.ir

مهلت تحویل: نیمه‌شب سه‌شنبه ۱۷ دی

راه‌اندازی ابزار Spin

در این تمرین مدل‌سازی یک سیستم با زبان PROMELA و درستی‌یابی آن با ابزار Spin را تمرین خواهید کرد. برای بارگیری Spin می‌توانید به راهنمای آن در آدرس `http://spinroot.com/spin/Man/README.html` مراجعه کنید یا از دستورهای `sudo apt-get install spin` (در Ubuntu Linux) یا `brew install spin` (در macOS با HomeBrew) استفاده کنید.

برای راحتی کار می‌توانید از رابط‌های گرافیکی‌ای که روی Spin طراحی شده‌اند مانند iSpin[۱] و jSpin[۲] نیز کمک بگیرید. توجه داشته باشید که در انتها باید کد خود را با قالب `.pml` به عنوان پاسخ بارگذاری کنید.

توصیه می‌شود از ویرایشگرهای معمول و افزونه‌های[۳] آن‌ها برای توسعهٔ کد خود استفاده کنید.

مدل‌سازی و درستی‌یابی صوری یک دستگاه فروش خودکار

یک نمونه از جایگزینی کسب‌وکارهای سنتی با مدل‌های جدید کسب‌وکار، فراگیر شدن *دستگاه‌های فروش خودکار*[۴] به عنوان بقالی‌های مدرن و خودکار است.

یک دستگاه فروش خودکار معمولاً به همراه یک *کارت‌خوان*[۵] کار می‌کند. مشتری با انتخاب محصول موجود در دستگاه فروش و پرداخت هزینهٔ آن از طریق کارت‌خوان محصول را دریافت می‌کند.

اما این دستگاه‌ها هم مانند هر سیستم دیجیتالی دیگری مشکلات خودشان را دارند!

۱ مدل‌سازی سیستم

به طور دقیق‌تر، برای خرید یک محصول در دستگاه خرید خودکار مدل ECE-VM این اتفاق‌ها رخ می‌دهند:

۱. مشتری محصول مورد نظرش را به دستگاه فروش خودکار اعلام می‌کند.

---

[۱] نیازمند Tcl/Tk Wish
[۲] نیازمند Java
[۳] مانند Sublime-Promela-Spin، language-promela for Atom، code-spin for VSCode و Promela for VS Code
[4] Vending Machines
[5] POS

۲. دستگاه قیمت محصول را از طریق شبکه به کارت‌خوان اعلام می‌کند.

۳. مشتری هزینه را پرداخت می‌کند.

۴. کارت‌خوان از طریق شبکه نتیجهٔ پرداخت (*پرداخت موفقیت‌آمیز بود.*) را به دستگاه فروش اعلام می‌کند.

۵. دستگاه محصول را به مشتری تحویل می‌دهد.

در این بین ممکن است اتفاقات دیگری نیز رخ دهد؛ مثلاً:

- پس از مورد ۱ محصول موجود نباشد.
- در مورد ۳ مشتری خرید را از طریق دستگاه خرید لغو کند. پس از لغو، دستگاه خرید به حالت اولیه باز می‌گردد و کارت‌خوان از لغو درخواست مطلع نمی‌شود.
- در مورد ۳ مشتری پرداخت را از طریق کارت‌خوان لغو کند. پس از لغو، کارت‌خوان به حالت اولیه باز می‌گردد و دستگاه خرید از لغو درخواست مطلع نمی‌شود.
- در مورد ۳ ارتباط با بانک با مشکل مواجه شود یا مشتری موجودی کافی نداشته باشد. در این حالت دستگاه خرید از این مسأله مطلع نمی‌شود و همچنان منتظر پاسخ *پرداخت موفقیت‌آمیز بود.* می‌ماند.
  در این صورت مشتری ممکن است پرداخت را تکرار کند.
- در مورد ۵ محصول در دستگاه گیر کند.

سیستمی را که از یک دستگاه خرید خودکار، یک کارت‌خوان و یک مشتری تشکیل می‌شود با PROMELA مدل‌سازی کنید.
برای ساده‌سازی مدل از این فرض‌ها استفاده کنید:

- دستگاه فقط دو محصول دارد: اسپرایت و کوکاکولا.
- موجودی هر محصول نامحدود است.
- محصول در دستگاه گیر نمی‌کند.
- موجودی حساب مشتری نامحدود است.
- نیازی به مدل‌سازی زیرساخت بانکی نیست. عدم توانایی ارتباط با بانک را می‌توانید در خود کارت‌خوان مدل‌سازی کنید.
- برای مدل‌سازی ارتباطات تحت شبکه (ارتباط کارت‌خوان با دستگاه خرید و برعکس) از یک کانال با ظرفیت ۱ استفاده کنید.
  سایر ارتباطات را با کانال‌هایی با مدل ارتباطی قرار ملاقات[۶] مدل‌سازی کنید.
- هر کدام از پردازه‌ها ممکن است چندین بار اجرا شوند. (می‌توانید از `do` استفاده کنید.)
- اگر کاربر سفارش را در یکی از دو دستگاه کارت‌خوان یا دستگاه خرید لغو کند، دستگاه دیگر لزوماً مطلع نمی‌شود. به عبارت دیگر، دستگاه‌ها لغو درخواست را به یکدیگر اطلاع نمی‌دهند.

بررسی کنید که مدل شما دچار بن‌بست[۷] می‌شود یا نه.

[6] rendezvous
[7] deadlock

۲ درستی‌یابی صوری

برای بررسی صحت سیستم، برقرار بودن ویژگی‌های زیر را در آن بررسی می‌کنیم:

دریافت محصول درست همواره چنین است که اگر محصولی دریافت شود، از همان نوعی است که آخرین بار سفارش داده شده است.

دریافت محصول پس از پرداخت همواره چنین است که اگر پرداخت جدیدی صورت گیرد در نهایت محصولی دریافت می‌شود.

هزینهٔ پرداختی درست همواره چنین است که اگر محصولی دریافت شود آخرین پرداخت برابر قیمت آن محصول بوده است.

برای هر یک از ویژگی‌های مذکور،

- در گزارش خود بررسی کنید که آن ویژگی یک ویژگی سرزندگی[۸]، ایمنی[۹] و ناوردایی[۱۰] است یا نه.
- با تبدیل این ویژگی‌ها به توصیف LTL، بررسی کنید که سیستم شما آن ویژگی را ارضا می‌کند یا نه. اگر ویژگی ارضا نمی‌شود در گزارشتان یک مثال نقض برای آن ویژگی ارائه دهید.

نحوهٔ تحویل

لطفاً فقط کد نهایی خود (شامل کد PML توصیف مدل و توصیف LTL ویژگی‌ها) و نسخهٔ PDF گزارش خود را در پرونده‌ای به نام `SID.zip` (که SID شمارهٔ دانشجویی شماست) پیش از اتمام مهلت تحویل در صفحهٔ وب درس بارگذاری کنید. سعی کنید ضمن پاسخ به سؤالت مطرح‌شده، گزارش خود را بسیار مختصر (حداکثر یک صفحه) بنویسید. همچنین، لطفاً کدتان را خوانا بنویسید و معیارهای تمیزی کد را رعایت کنید.

توجه داشته باشید که این تمرین تحویل حضوری دارد و در صورت حضور نیافتن در تحویل حضوری نمره‌ای از این تمرین دریافت نخواهید کرد.

[8] liveness
[9] safety
[10] invariant