



## دانشگاه تهران

پردیس دانشکده‌های فنی  
دانشکده مهندسی برق و کامپیوتر

### عنوان

بررسی روش‌های تجرید مدل‌های ربکا به منظور درستی‌یابی صوری

### نگارش

حمیده صبوری قمی

### استاد راهنما

دکتر مرجان سیرجانی

### استاد مشاور

دکتر رامتین خسروی

پایان‌نامه برای دریافت درجه کارشناسی ارشد در رشته

مهندسی کامپیوتر-گرایش نرم‌افزار

شهریور ماه ۱۳۸۷







بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



## تعهد نامه اصالت اثر

اینجانب حمیده صبوری قمی تأیید می کنم که مطالب مندرج در این پایان نامه حاصل کار پژوهشی اینجانب است و به دستاوردهای پژوهشی دیگران که در این نوشته از آنها استفاده شده است مطابق مقررات ارجاع گردیده است. این پایان نامه قبلاً برای احراز هیچ مدرک هم سطح یا بالاتر ارائه نشده است. کلیه حقوق مادی و معنوی این اثر متعلق به دانشکده فنی دانشگاه تهران می باشد.

نام و نام خانوادگی دانشجو: حمیده صبوری قمی  
امضای دانشجو:









## چکیده

استفاده از درستی‌یابی صوری رهیافتی مطمئن برای ایجاد سیستم‌های قابل اطمینان است. از طرفی درستی‌یابی سیستم‌های بزرگ به دلیل انفجار فضای حالت با مشکل مواجه است. بنابراین برای بهره‌مندی از مزایای درستی‌یابی در این سیستم‌ها لازم است که ابتدا این مشکل رفع شود. استفاده از روش‌های تجرید مدل در درستی‌یابی یکی از راه‌های مقابله با مشکل انفجار فضای حالت است. تجرید داده، تجرید براساس تفسیر مجرد، تجرید گزاره، درستی‌یابی پیمانه‌ای و برش دادن نمونه‌هایی از روش‌های تجرید مدل می‌باشند. در میان این روش‌ها، برش دادن برنامه به دلیل خودکار بودن، حفظ ویژگی‌های مدل به صورت قوی و قابل ترکیب بودن با دیگر روش‌های تجرید، روش مناسبی برای تجرید مدل خواهد بود. برای برش دادن یک مدل باید ابتدا آن مدل از نظر جریان کنترل و جریان داده تحلیل شود. حاصل تحلیل جریان کنترل مدل‌ها گراف جریان کنترل است که از آن برای تحلیل داده استفاده می‌شود. در قدم بعدی یک گراف وابستگی برای مدل تولید می‌شود که نشان‌دهنده وابستگی‌های موجود میان جملات مدل است. در مرحله نهایی با اعمال یک الگوریتم دسترس‌پذیری روی این گراف یک برش از مدل بدست می‌آید.

در این پایان‌نامه در ابتدا تکنیک برش دادن ایستا برای مدل‌های ربکا ارائه شده است. ربکا یک زبان مبتنی بر اکتور است که برای مدلسازی سیستم‌های همروند استفاده می‌شود. برای تحلیل جریان کنترل مدل‌های ربکا، گراف‌های جریان کنترل ربکا و جریان کنترل تخمینی ربکا معرفی شده‌اند. برای مدلسازی وابستگی‌های موجود میان جملات مدل‌ها، گراف وابستگی ربکا و گراف وابستگی مبتنی بر ربکا ارائه شده‌اند. این گراف‌ها (جریان کنترل و وابستگی) منطبق بر مفاهیم معنایی زبان ربکا می‌باشند.

از آنجایی که برش دادن ایستا معمولاً برش‌های بزرگی از مدل ایجاد می‌کند، دو تکنیک جدید برش دادن قدم به قدم و برش دادن کراندار، در این پایان‌نامه پیشنهاد شده‌اند. برش دادن قدم به قدم در ابتدا حد بالایی از مدل را به عنوان برش محاسبه می‌کند و در مراحل بعد براساس نتیجه درستی‌یابی (برقراری یا نقض ویژگی و مثال نقض تولید شده) برش را پالایش می‌کند. برش دادن کراندار با استفاده از جملات تخصیص غیرقطعی در ربکا، حدودی را برای الگوریتم برش مشخص می‌کند. همچنین در این پایان‌نامه یک تکنیک ساده برای برش دادن مدل‌ها برای تشخیص بن‌بست نیز پیشنهاد شده است (تکنیک‌های دیگر برش دادن، یک برش از مدل را برای بررسی یک ویژگی خاص محاسبه می‌کنند).

در انتها نیز کاربردی بودن تکنیک‌های معرفی شده با اعمال آنها روی تعدادی مثال و ارائه نتایج بدست آمده، نشان داده شده است.







## فهرست مطالب

۲	..... مقدمه	۱
۶	..... ربکا	۱-۱
۹	..... ساختار پایان نامه	۲-۱
۱۳	..... روش‌های تجرید	۲
۱۵	..... تجرید داده	۱-۲
۱۷	..... تفسیر مجرد	۲-۲
۱۹	..... تجرید گزاره	۳-۲
۲۱	..... درستی‌یابی پیمانهای	۴-۲
۲۲	..... برش دادن برنامه	۵-۲
۲۶	..... برش دادن برنامه	۳
۲۸	..... تحلیل درون رویه‌ای برنامه‌های ترتیبی	۱-۳
۲۸	..... تحلیل جریان کنترل	۱-۱-۳
۳۱	..... تحلیل جریان داده	۲-۱-۳
۳۴	..... گراف وابستگی برنامه	۳-۱-۳
۳۶	..... الگوریتم برش دادن	۴-۱-۳
۳۸	..... تحلیل برنامه‌های همروند	۲-۳
۳۸	..... گراف جریان کنترل	۱-۲-۳
۴۰	..... گراف وابستگی برنامه	۲-۲-۳
۴۲	..... الگوریتم برش دادن	۳-۲-۳
۴۴	..... تحلیل برون رویه‌ای برنامه‌ها	۳-۳
۵۱	..... کارهای مشابه	۴
۵۷	..... تجرید مدل‌های ربکا با استفاده از برش دادن	۵
۵۸	..... تحلیل جریان کنترل	۱-۵

۶۰	مدلسازی فراخوانی پیغام‌پردازها	۱-۱-۵
۶۴	تحلیل جریان داده	۲-۵
۶۷	گراف وابستگی ربکا	۳-۵
۶۸	وابستگی کنترلی و داده میان جملات	۱-۳-۵
۷۰	پیغام‌پردازها و تبادل پیغام	۲-۳-۵
۷۱	کلاس‌های واکنشی	۳-۳-۵
۷۲	گراف وابستگی مبتنی بر ربکا	۴-۵
۷۷	تعریف برش	۵-۵
۷۸	الگوریتم‌های برش دادن مدل‌های ربکا	۶-۵
۷۹	الگوریتم برش دادن ایستا	۱-۶-۵
۸۱	الگوریتم برش دادن ایستا بدون توجه به یک ویژگی خاص	۲-۶-۵
۸۲	الگوریتم برش دادن قدم به قدم	۳-۶-۵
۸۵	الگوریتم برش دادن کراندار	۴-۶-۵
۹۲	۶ اعمال روش‌های پیشنهادی بر بررسی‌های موردی	
۹۲	مساله توافق	۱-۶
۹۳	فلاسفه گرسنه	۲-۶
۹۴	فرستنده و گیرنده	۳-۶
۹۵	پردازنده	۴-۶
۹۶	خط تولید	۵-۶
۹۷	ساعت	۶-۶
۹۸	آرایشگر خواب‌آلود	۷-۶
۹۹	پروتکل ارسال مجدد کراندار	۸-۶
۱۰۱	جمع‌بندی نتایج	۹-۶
۱۰۵	نتیجه‌گیری	۷



- ۸ فهرست منابع ..... ۱۰۸
- فرهنگ واژگان (انگلیسی به فارسی) ..... ۱۱۲
- فرهنگ واژگان (فارسی به انگلیسی) ..... ۱۱۹

## فهرست اشکال

- شکل ۱-۲: یک مدل ساده شامل یک فرستنده و یک گیرنده در ربکا ..... ۷
- شکل ۱-۳: یک کلاس واکنشی در ربکا و کلاس واکنشی مجرد آن ..... ۱۷
- شکل ۲-۳: یک کلاس واکنشی و کلاس واکنشی مجرد آن با استفاده از گزاره  $(lastMsg == newMsg)$  ..... ۲۰
- شکل ۱-۴: مراحل ایجاد یک برش از برنامه ..... ۲۷
- شکل ۲-۴: یک برنامه نمونه و گراف جریان کنترل آن ..... ۲۹
- شکل ۳-۴: یک گرامر ساده به همراه محاسبه  $def$  و  $ref$  برای آن ..... ۳۰
- شکل ۴-۴: یک برنامه ساده به همراه گراف وابستگی برنامه ..... ۳۶
- شکل ۵-۴: گراف وابستگی برنامه و کد برنامه پس از برش دادن یک برنامه ساده نسبت به جمله ۱۰ ..... ۳۸
- شکل ۶-۴: یک برنامه ساده به همراه گراف جریان کنترل ریسمان‌های آن ..... ۳۹
- شکل ۷-۴: یک مثال برای نشان دادن عدم وجود خاصیت تعدی در یال‌های وابستگی مداخله‌ای ..... ۴۲
- شکل ۸-۴: یک برنامه نمونه به همراه گراف وابستگی سیستم آن ..... ۴۶
- شکل ۱-۵: یک قطعه کد شامل انتخاب غیرقطعی در پروملا و گراف وابستگی برنامه‌ی مربوط به آن ..... ۵۱
- شکل ۲-۵: یک برنامه نمونه به همراه برش دادن نمونه‌ی آن برای پاسخ به سوال اول و سوال دوم ..... ۵۳
- شکل ۱-۶: گراف جریان کنترل با دو خروجی و بدون خروجی و گراف جریان کنترل معادل آنها با یک خروجی ..... ۵۸
- شکل ۲-۶: نمایش کلی از مدلسازی فراخوانی پیغام‌ها در گراف جریان کنترل ربکا ..... ۶۰
- شکل ۳-۶: تعدادی پیغام‌پرداز موجود در یک مدل و گراف جریان کنترل ربکا بدست آمده به کمک روش اول ... ۶۱
- شکل ۴-۶: تعدادی پیغام‌پرداز و گراف جریان کنترل ربکا ..... ۶۳
- شکل ۵-۶: گراف جریان کنترل ربکا برای مدل فرستنده و گیرنده ..... ۶۴
- شکل ۶-۶: محاسبه تعاریف در دسترس برای جملات مدل فرستنده و گیرنده ..... ۶۷
- شکل ۷-۶: دو پیغام‌پرداز و وابستگی‌های داده و وابستگی‌های داده درون‌ربکا میان آنها ..... ۶۹
- شکل ۸-۶: دو ریسمان و وابستگی‌های داده و وابستگی‌های مداخله میان آنها ..... ۷۰
- شکل ۹-۶: گراف وابستگی ربکا برای مدل فرستنده و گیرنده ..... ۷۲
- شکل ۱۰-۶: یک مدل ربکا شامل یک فرستنده و دو گیرنده ..... ۷۴
- شکل ۱۱-۶: گراف وابستگی ربکا برای یک مدل ربکا با یک فرستنده و دو گیرنده ..... ۷۵
- شکل ۱۲-۶: گراف وابستگی مبتنی بر ربکا برای یک مدل ربکا با یک فرستنده و دو گیرنده ..... ۷۶
- شکل ۱۳-۶: گراف وابستگی ربکا برای مدل فرستنده و گیرنده پس از برش دادن نسبت به بن‌بست ..... ۸۲
- شکل ۱۴-۶: مراحل تکنیک پالایش با راهنمایی مثال نقض ..... ۸۳
- شکل ۱۵-۶: برش مدل فرستنده و گیرنده پس از برش دادن کراندار با در نظر گرفتن مجموعه متغیر  $\{msg\}$  ... ۸۸

## فهرست جداول

جدول ۱-۳: مقایسه روش‌های تجرید .....	۱۱
جدول ۱-۶: تعریف توابع <i>def</i> و <i>ref</i> برای جملات زبان ریکا .....	۶۶
جدول ۲-۶: مقادیر دو تابع <i>def</i> و <i>ref</i> برای جملات مدل فرستنده و گیرنده .....	۶۶
جدول ۱-۷: نتایج درستی‌یابی مساله توافق .....	۹۳
جدول ۲-۷: نتایج درستی‌یابی مدل فلاسفه گرسنه .....	۹۴
جدول ۳-۷: نتایج درستی‌یابی مدل فرستنده و گیرنده .....	۹۵
جدول ۴-۷: نتایج درستی‌یابی پردازنده .....	۹۶
جدول ۵-۷: نتایج درستی‌یابی مدل خط تولید .....	۹۷
جدول ۶-۷: نتایج درستی‌یابی مدل ساعت .....	۹۸
جدول ۷-۷: نتایج درستی‌یابی مدل آرایشگر خواب‌آلود .....	۹۹
جدول ۸-۷: نتایج درستی‌یابی پروتکل ارسال مجدد کراندار .....	۱۰۱

