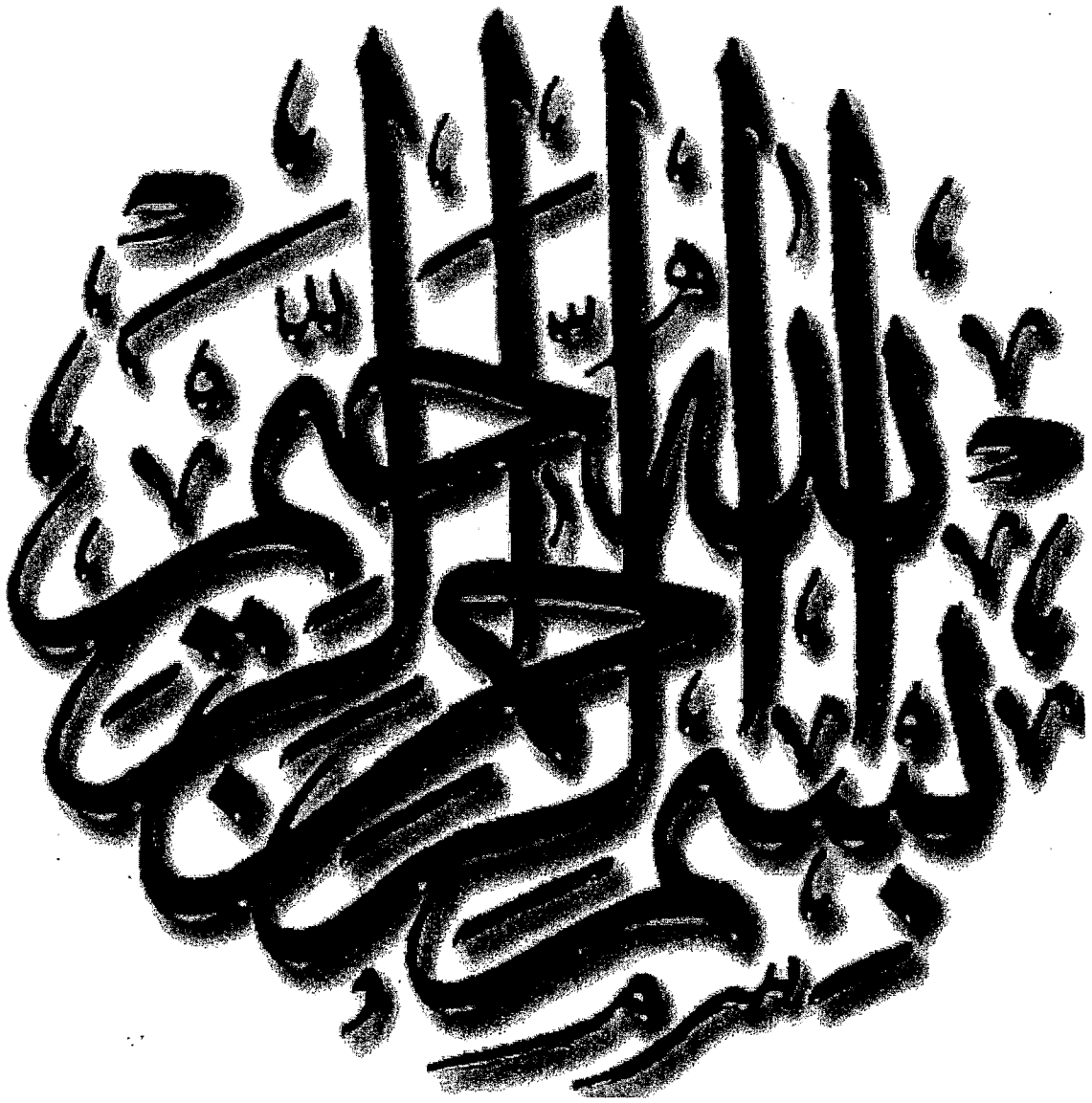
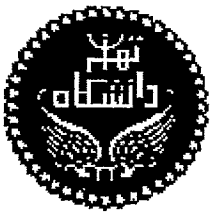
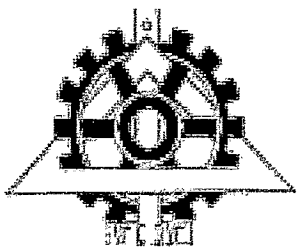






دانشگاه تهران

پردیس دانشکده‌های فنی

دانشکده مهندسی برق و کامپیوتر

عنوان:

درستی‌یابی صوری سیستم‌های شیءبنیاد توسط جبر پردازه‌ای

نگارش:

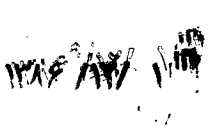
حسین حجت

استاد راهنما:

دکتر مرجان سیرجانی

استاد مشاور:

دکتر ناصر یزدانی



پایان‌نامه برای دریافت درجهٔ کارشناسی ارشد در رشته

مهندسی کامپیوتر-گرایش نرم‌افزار

آبان ماه ۱۳۸۶

به نام خدا

دانشگاه تهران

پردیس دانشکده های فنی

دانشکده مهندسی برق و کامپیوتر

گواهی دفاع از پایان نامه کارشناسی ارشد

هیأت داوران پایان نامه کارشناسی ارشد آقا/خانم حسین حجت در رشته مهندسی برق و کامپیوتر، گرایش : نرم افزار

با عنوان: "درستی یابی صوری سیستمهای شی ء بنیاد توسط جبر پردازه ای"

در تاریخ ۱۳۸۶/۰۸/۲۳ نمره نهایی پایان نامه: به عدد ۱۹,۸ به حروف نوزده و هشت دهم

و درجه عالی ارزیابی نمود.

مشخصات هیأت داوران	نام و نام خانوادگی	مرتبه دانشگاهی	دانشگاه یا موسسه	امضاء
۱-استاد راهنما استاد راهنمای دوم (حسب مورد)	دکتر مرجان سیرجانی	استادیار	تهران	
۲-استاد مشاور	دکتر ناصر یزدانی	دانشیار	تهران	
۳-استاد مدعو خارجی (یا استاد مشاور دوم)	دکتر سید حسن میریان	استادیار	شریف	
۴-استاد مدعو داخلی	دکتر رامتین خسروی	استادیار	تهران	
۵-داور و نماینده کمیته تحصیلات تکمیلی دانشکده	دکتر فتانه تقی یاره	استادیار	تهران	

تذکر:این برگه پس از تکمیل توسط هیأت داوران در نخستین صفحه پایان نامه درج می گردد.

تحصیلات تکمیلی

دانشگاه تهران

پردیس دانشکده‌های فنی

دانشکده مهندسی برق و کامپیوتر

عنوان:

درستی‌یابی صوری سیستم‌های شیءبنیاد توسط جبر پردازه‌ای

نگارش: **حسین حجت**

پایان‌نامه جهت دریافت درجه کارشناسی ارشد در رشته

مهندسی کامپیوتر گرایش نرم‌افزار

از این پایان‌نامه در تاریخ ۱۳۸۶/۸/۲۳ در مقابل هیأت داوران دفاع به عمل آمد و مورد تصویب قرار گرفت.

معاونت آموزشی تحصیلات تکمیلی پردیس دانشکده‌های فنی:	دکتر جواد فیض
رییس دانشکده مهندسی برق و کامپیوتر:	دکتر پرویز جبه‌دار مارالانی
معاونت پژوهشی و تحصیلات تکمیلی دانشکده:	دکتر سعید نادر اصفهانی
استاد راهنما:	دکتر مرجان سیرجانی
استاد مشاور:	دکتر ناصر یزدانی
عضو هیأت داوران:	دکتر فتانه تقی‌یاره
عضو هیأت داوران:	دکتر رامتین خسروی
عضو هیأت داوران:	دکتر سید حسن میریان حسین‌آبادی

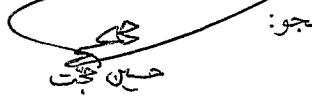
تعهد نامه اصالت اثر

اینجانب **حسین حجت** تأیید می‌کنم که مطالب مندرج در این پایان‌نامه 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 می‌باشد.

نام و نام خانوادگی دانشجو: **حسین حجت**

امضای دانشجو:



تقدیم به ساحت مقدس یوسف زهرا (عج)

تشکر و قدردانی:

خداوند یکتا را سپاس می‌گویم که به من امکان داد تا بتوانم قدمی دیگر از راه پر پیچ و خم کسبِ دانش را با موفقیت پشت سر بگذارم. آرزو می‌کنم که در ادامه‌ی مسیر بتوانم شایسته‌ی رحمت بیکرانش باشم.

در پیمودن این راه، افراد بسیاری نیز همواره راهنما و یاری‌رسان من بودند، که از همگی آنان سپاسگزارم. ابتدا از استاد راهنمای بزرگوارم دکتر مرجان سیرجانی کمال تشکر را دارم، که در طی سال‌ها عضویت در گروه تحقیقاتی ایشان–چه در دوره‌ی کارشناسی و چه در دوره‌ی کارشناسی ارشد– تجربیات گرانبهایی اندوختم. امیدوارم که این همکاری تا سال‌های سال ادامه یابد. از استاد مشاورم دکتر ناصر یزدانی تشکر می‌کنم که به خوبی مرا در خلال این پروژه یاری کردند. از دوست عزیزم دکتر محمدرضا موسوی نیز قدردانی می‌کنم، که در کلیه‌ی مراحل انجام پروژه کمک و راهنمای من بودند. همچنین از کلیه‌ی دوستان و عزیزان آزمایشگاه روش‌های صوری نیز کمال تشکر و قدردانی را دارم.

و در آخر، از داناترین و مهربان‌ترین راهنمای زندگی‌ام، پدرم، از بهترین و دلسوزترین یار زندگی‌ام، مادرم، و دو خواهر عزیز و نازنینم تشکر می‌کنم که هر چه دارم از برکت تلاش‌ها، زحمات و دعاهای بی‌دریغ آنان است. حق حافظ و نگهدارشان باد.

چکیده

الگوی مبتنی بر شیء یکی از رایج‌ترین رویکردها به برنامه‌سازی و مدل‌سازی است. باوجود اینکه پیشرفت‌های بسیاری در این زمینه انجام شده است، اما به نظر می‌رسد که هنوز این الگو نظریات پخته و جاافتاده‌ای برای استدلال صوری نداشته باشد. در این پایان‌نامه تلاش می‌کنیم که پایه‌ای برای استدلال صوری در زمینه‌ی زبان‌های مبتنی بر شیء بنا کنیم. برای تحلیل صوری، از شیوه‌ی تحلیل جبرپردازه‌ای استفاده می‌کنیم، که رویکردی قدرتمند برای مدل‌سازی سیستم‌های همروند است. با فراهم کردن نگاشتی از زبان‌های مبتنی بر شیء به جبرپردازه‌ای، می‌توانیم از توانمندی‌های جبرپردازه‌ای در کاربردهای صنعتی نیز استفاده کنیم. در نگاشت ارائه شده به طور خاص بر جبرپردازه‌ای mCRL2 تمرکز می‌کنیم، که یک شکل از جبرهای پردازه‌ای است که از انواع داده‌ای به خوبی پشتیبانی می‌کند. توانایی‌های mCRL2 در کارهای بسیاری پیش از این به اثبات رسیده بودند، و علاوه‌براین مجموعه ابزارهای نیرومندی برای تحلیل و درستی‌یابی مدل‌های mCRL2 وجود دارند.

برای عملی کردن ایده‌های خود از دو زبان مبتنی بر شیء استفاده می‌کنیم. اولی زبان ربکاست، که زبانی مبتنی بر مدل بازیگر است که برای مدل‌سازی سیستم‌های همروند و توزیع‌شده به کار می‌رود. زبان دوم زبان SystemC است که در صنعت کاربرد بسیار دارد. این زبان در طراحی‌های در سطح سیستم کاربرد دارد.

برتری‌های رویکرد ما در مقایسه با نگاشت‌های انجام شده‌ی پیشین در زمینه‌ی تبدیل زبان‌های مبتنی بر شیء به جبرپردازه‌ای، استفاده‌ی بسیار از انواع داده‌ای موجود در mCRL2 است. توانایی انواع داده‌ای موجود در mCRL2 تاحدی بود که عموماً نیازی به تعریف مجدد انواع داده‌ای احساس نشد. هر دو نگاشت در قالب یک ابزار کامپایلر پیاده‌سازی شده و تعدادی مطالعه‌ی موردی در هر دو مورد انجام شده‌اند. نتایج نگاشت ربکا نشان می‌دهد که کاهش ترتیب جزئی پویا اندازه‌ی فضای حالت را نسبت به روش‌های پیشین (که ایستا بودند) بیشتر کاهش می‌دهد، حال آنکه از لحاظ زمانی کُندتر است. همچنین توانستیم که یک اشکال در پیاده‌سازی انجام شده‌ی قبلی برای روش‌های ایستای کاهش ترتیب جزئی بیابیم، که توسط خوشه‌سازی قابل حل شدن است. در نگاشت SystemC نیز یک اشکال مخفی در پیاده‌سازی ریزپردازنده‌ی mini MIPS پیدا شد، که تا قبل از آن یافته نشده بود.

فهرست مطالب

عنوان..... صفحه

فهرست شکل‌ها

عنوان..... صفحه

فهرست جدول‌ها

عنوان..... صفحه

فصل اول

مقدمه

در حوزه‌ی دانش کامپیوتر، "روش‌های صوری"[1] به روش‌هایی مبتنی بر ریاضیات اطلاق می‌شوند که در توصیف، طراحی و درستی‌یابی سیستم‌ها مورد استفاده قرار می‌گیرند. به کار بردن روش‌های صوری درک بیشتر و دقیق‌تری از سیستم می‌دهد و موجب افزایش وضوح توصیف می‌شود. علاوه براین در زدودن اشکالات و خطاهای موجود در سیستم کمک شایانی می‌کند.

روش‌های صوری مختلف بر روی سیستم‌های متفاوتی تمرکز دارند. به طور کلی سیستم‌های محاسباتی به دو شاخه‌ی ترتیبی[2] و واکنشی[3] تقسیم می‌شوند. محاسبات در نوع اول به صورت یک تابع ورودی- خروجی است؛ ورودی از یک سمت وارد محاسبه‌گر شده خروجی به صورت تابعی از ورودی از سمت دیگر بیرون داده می‌شود. برای چنین سیستم‌هایی، روش‌های صوری مختلفی نظیر حساب لاندا (Barendregt 1984) ارائه شده‌اند. طبق نظریه‌ی چرچ-تورینگ هیچ مدل محاسباتی برای یک سیستم ترتیبی نمی‌تواند قدرت بیشتری از ماشین تورینگ داشته باشد.

برخلاف مدل ترتیبی، یک سیستم واکنشی در تعامل دائمی با محیط اطراف خود است و هیچ‌گاه به اتمام نمی‌رسد. در چنین وضعیتی سیستم به طور همروند با محیط اطراف خود اجرا می‌شود. نمونه‌ی بارز چنین رفتاری را در یک سیستم‌عامل می‌توان دید، که با مشاهده‌ی اتفاقات مختلف پیش آمده در کامپیوتر به آنها پاسخ می‌دهد. در بررسی سیستم‌های واکنشی نمی‌توان تنها به صورت مجرد ورودی-خروجی اکتفا نمود. یک رویکرد صوری درست به این سیستم‌ها باید الگوهای رفتاری سیستم، وقوع بن‌بست، قحطی[4] و نظائر آن را در نظر داشته باشد. بسته به پارامترهای رفتار/سیستم، درهم‌سازی[5]/عدم درهم‌سازی، خطی/ انشعابی بودن زمان، مدل‌های متفاوتی را می‌توان برای یک سیستم همروند در نظر گرفت (Sassone, Nielsen et al. 1996).

جبرپردازه‌ای، یکی از موفق‌ترین مدل‌های صوری در توصیف سیستم‌های همروند است. نگرش

---

[1] Formal Methods
[2] Sequential
[3] Reactive
[4] Starvation
[5] Interleaving

جبری به پردازه‌های موازی در دهه‌ی هفتاد با معرفی "پردازه‌های ترتیبی مرتبط"[1] توسط تونی هُر[2] (Hoare 1978; Hoare 1985) و نیز "حساب سیستم‌های مرتبط"[3] توسط رابین میلنر[4] (Milner 1980; Milner 1989) آغاز شد. برای اولین بار یان برخسترا[5] و یان ویلم کلاپ[6] در "جبر پردازه‌های مرتبط"[7] به این شیوه از مدل‌سازی سیستم‌های همروند نام "جبر پردازه‌ای" دادند (Bergstra and Klop 1984; Baeten and Weijland 1990)، که تا امروز نیز به کار برده می‌شود. سه جبر پردازه‌ای نامبرده در فوق، اصلی‌ترین رویکردهای موجود هستند و باقی جبر پردازه‌ها معمولاً در موارد خاص به کار گرفته می‌شوند، مثل حساب پای[8] (Milner 1999; Sangiorgi and Walker 2001) برای سیستم‌های متحرک و PEPA (Hillston 1996) برای توصیف سیستم‌های اتفاقی. در خلال این پایان‌نامه، از نام‌های مختصر جبرهای پردازه‌ای CCS، CSP و ACP استفاده خواهیم نمود.

در نام هر سه جبر پردازه‌ای نامبرده، بر روی ارتباط تأکید شده است. علت این نام‌گذاری از آنجا ناشی می‌شود که در جبر پردازه‌ای، هدف توصیف و استدلال در زمینه‌ی سیستم‌های مرتبط است. چنین سیستم‌هایی از طریق یک سری ارتباطات با جهان اطراف خود کنش دارند. در جبر پردازه‌ای از محاسبات داخلی درونی هر پردازه (متغیرها، تخصیص دادن مقدار به متغیر،...) کلاً صرف‌نظر می‌شود. به عبارت دیگر یک دید سطح بالا به سیستم وجود دارد، که تمامی سیستم‌های مرتبط را به صورت مجرد پردازه می‌بیند، به طوری که هر پردازه عضوی از یک دامنه‌ی ریاضی است. پردازه‌ها توسط یک سری عملگر قابل ترکیبند. برای مثال، عملگرهایی برای ترکیب ترتیبی و یا موازی پردازه‌ها وجود دارند. قواعدی نیز در هر جبر پردازه‌ای باید وجود داشته باشند که نحوه‌ی عمل عملگرها را مقید کنند، تا هر عملگر مطابق آنچه که از آن انتظار می‌رود عمل کند. بنابراین هر جبر پردازه‌ای شامل یک دامنه از پردازه‌ها به همراه یک

---

[1] Communicating sequential processes (CSP)
[2] Sir Charles Antony Richard Hoare (CAR Hoare)
[3] Calculus of communicating systems (CCS)
[4] Robin Milner
[5] Jan Bergstra
[6] Jan Willem Klop
[7] Algebra of Communicating Processes (ACP)
[8] Pi-Calculus

مجموعه عملگرهایی است که در قواعد خاصی صدق می‌کنند.

مدل‌های صوری بسیاری وجود دارند که برخلاف جبر پردازه‌ای، به پردازه‌ها دید مجرد ندارند. به عنوان مثال در این زمینه، می‌توان به شبکه‌های پتری (Murata 1989) اشاره کرد. شبکه‌های پتری، پردازه‌ها را جزئی‌تر و عینی‌تر از جبر پردازه‌ها توصیف می‌کنند (Olderog 1991)؛ حال آنکه در جبر پردازه‌ای پردازه‌ها موجوداتی مجردند و تأکید بر نحوه‌ی ترکیب آنهاست. در شبکه‌های پتری، رابطه‌های علّی مابین وقوع رخدادها و همروندی صحیح قابل بیان است، ولی توصیف سیستم‌های واقعی و بزرگ به دلیل نداشتن ساختارهایی مانند جبر پردازه‌ای در آنها مشکل است. در این پایان‌نامه مدل صوری مورد استفاده جبر پردازه‌ای است. یکی از دلائل این انتخاب، وجود ابزارهای پشتیبان قدرتمند برای جبر پردازه‌ای استفاده شده است که در فصل‌های آتی به آنها اشاره خواهد شد.

جبر پردازه‌ای نه تنها به عنوان یک چارچوب برای استدلال صوری و استنتاج یک سری صفات از سیستم می‌تواند به کار رود، بلکه به عنوان یک ابزار برای درستی یابی[1] قابل استفاده است. منظور از درستی یابی در اینجا بدین معناست که به ازای تمامی ورودی‌های ممکن آیا خروجی صحیح و مورد نظر تولید می‌شود یا خیر. روند کلی درستی‌یابی به روش جبری را می‌توان به این صورت خلاصه کرد (Fokkink 2000). در ابتدا، پیاده‌سازی سیستم به صورت یک عبارت پردازه‌ای توصیف می‌شود. سپس، از بن‌بست برای مجبور کردن کنش‌ها به برقراری ارتباط استفاده می‌شود. از طریق کنش‌های خاموش[2] محاسبات درونی پنهان می‌شوند، به طوری که تنها ارتباط ورودی/خروجی از پیاده‌سازی باقی بماند. در نهایت، عبارت پردازه‌ای باقی‌مانده توسط منطق برابری[3] دستکاری می‌شود تا اثبات شود که سیستم همان رفتاری را دارد که از آن انتظار می‌رود. به عبارت صوری، فرض کنیم که سیستم از n مؤلفه‌ی موازی C_1، C_2، ... ، C_n تشکیل شده باشد. این مؤلفه‌ها ممکن است فرستنده، گیرنده، کانال ارتباطی و غیره باشند. همچنین H نشان‌دهنده‌ی مجموعه اعمال داخلی سیستم است که منجر به ارتباطات I می‌شود. اگر رفتار مورد نظر سیستم در قالب پردازه‌ی $Spec$ بیان شده باشد، آن‌گاه هدف از درستی‌یابی در جبر پردازه‌ای را

[1] Verification
[2] Silent action
[3] Equational logic

می‌توان به شکل رابطه‌ی زیر بیان کرد.

$$\tau_I(\partial_H(C_1||C_2 \cdots ||C_n)) = Spec$$

که درآن منظور از تساوی، یک شکل از هم‌ارزی[1] در جبر پردازه‌ای مثل "دوشباهت انشعابی"[2] است. در این فصل تنها یک شمای کلی از درستی‌یابی در جبر پردازه‌ای مورد تأکید است، و نمادهای استفاده شده در رابطه‌ی فوق در فصل‌های بعدی شرح داده شده‌اند.

توسط اصول موضوعی[3] جبرهای پردازه‌ای، می‌توان درستی رابطه‌ی فوق را در مورد سیستم‌های واقعی بررسی کرد. برای مثال، در فصل ششم مرجع (Milner 1989) درستی چندین مثال، از جمله پروتکل بیت متناوب[4] شرح داده شده است. در پیاده‌سازی این پروتکل، مؤلفه‌های فرستنده، گیرنده و کانال‌های ارتباطی برای ارسال و دریافت پیغام وجود دارند. همچنین، برای مدل کردن پایان زمان[5] یک شمارنده بایستی قرار داده شود. اما در توصیف رفتار پروتکل (سمت راست رابطه‌ی درستی‌یابی جبرپردازه‌ای)، هیچ‌یک از مؤلفه‌های کانال ارتباطی و شمارنده دیده نمی‌شوند. تنها کنش‌های مورد توجه در توصیف پروتکل این است که با فرستادن یک پیغام از طرف فرستنده، پیغام در سمت دیگر دریافت بشود. میلنر در این فصل از کتاب خود با استفاده از روابط موجود در CCS نشان داده که رابطه برای دوشباهت برقرار است، و پیاده‌سازی رفتار مورد انتظار را دارد.

در اوائل دهه‌ی ۹۰، مشخص شد که قدرت جبر پردازه‌ای در اثبات دستی مسائل محدود است، و نهایتاً منحصر به مسائلی در حد و اندازه‌ی پروتکل بیت متناوب می‌شود (Fokkink, Groote et al. 2004).یکی از اهداف تحقیق در حوزه‌ی جبر پردازه‌ای یافتن پاسخ به این سؤال بود که آیا می‌توان جبر پردازه‌ای را برای مسائل جدی‌تر و بزرگ‌تر استفاده کرد یا خیر. مقداری از این چالش در جبر پردازه‌ای لوتوس[6] (Tommaso and Ed 1987) پاسخ داده شده است. در لوتوس انواع داده‌ای و مقداری "شکر نحوی" به زبان اضافه شده‌اند. جبرپردازه‌ای دیگری که سعی در حل موضوع دارد، μCRL (Groote and

[1] Equiavalence
[2] Branching bisimilarity
[3] Axioms
[4] Alternating bit protocol
[5] Time-out
[6] LOTOS

Ponse 1994) است. μCRL نسبت به لوتوس ساده‌تر است، به طوریکه تنها با دو عملگر if-then-else و جمع در دامنه‌های نامتناهی انواع داده‌ای را به جبر پردازه‌ای اضافه کرده است. به دلیل توانایی بالا در بیان و درستی‌یابی سیستم‌ها، و نیز به خاطر دارا بودن ابزار پشتیبان قدرتمند، مدل صوری مورد استفاده در این پایان‌نامه، جبر پردازه‌ای μCRL و خصوصاً روایت جدید آن، mCRL2 (Groote, Mathijssen et al. 2005) است. مزیت mCRL2 نسبت به جبرهای پردازه‌ای که سابقاً در این زمینه به کار گرفته شده‌اند در موارد زیر قابل خلاصه کردن است:

۱. **وجود الگوریتم‌ها و تکنیک‌های قدرتمند کاهش.** جبرپردازه‌ای mCRL2 روش‌های توانمندی برای کاهش فضای حالت دارد، که در فصل هفتم این پایان‌نامه مورد بررسی قرار گرفته‌اند. یکی از علت‌های اصلی ترجمه‌ی زبان‌های مبتنی بر شیء به این جبرپردازه‌ای، استفاده کردن از این روش‌ها بوده است.

۲. **مناسب بودن زبان برای ترجمه.** نام جبرپردازه‌ای mCRL2 (micro Common Representation Language 2 یا خُرد زبان نمایش مشترکِ دو) است. صرف نظر از عدد ۲ که نشان‌دهنده‌ی روایت دوم زبان است، باقی نام بر این نکته اشاره دارد که یکی از اهداف اصلی در طراحی mCRL2 ساختن بنیانی برای نمایش زبان‌های گوناگون بوده است. برخوردار بودن از انواع داده‌ای غنی و توابع از پیش تعریف شده برای سروکار داشتن با این انواع داده‌ای در تبدیل زبان‌های مختلف به آن کمک شایانی می‌کند.

۳. **برخورداری از یک ابزار قدرتمند پشتیبانی.** هدف اصلی از درستی‌یابی به روش جبرپردازه‌ای اثبات کردن درستی سیستم توسط اصول موضوعه‌ی جبرپردازه‌ای است. اما با بزرگ شدن سیستم‌ها و دشوار شدن توصیف آنها، سروکار داشتن مستقیم با روابط مشخص کننده‌ی آنها کاری سخت و دشوار است. برای این منظور، یک ابزار پشتیبان برای این جبرپردازه‌ای طراحی شده است که بسیاری از اعمال مورد نیاز نظیر خطی‌سازی، تولید فضای حالت و کاهش را انجام می‌دهد.

۴. **جدید بودن زبان و فعال بودن جامعه‌ی پژوهشگران.** نظریه‌ها و ابزار قدرتمندی برای زبان mCRL2 ساخته شده‌اند و هنوز کارهای بسیاری در زمینه‌ی پیشبرد زبان در حال انجام است.