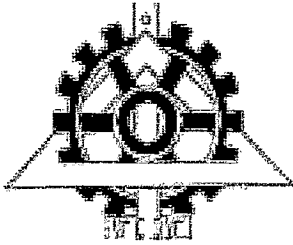


۹۲۰۲۹



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:

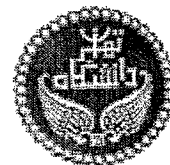
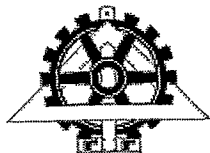
دکتر ناصر یزدانی

پایان‌نامه برای دریافت درجه کارشناسی ارشد در رشته

مهندسی کامپیوتر-گرایش نرم‌افزار

آبان ماه ۱۳۸۶

۹۳۰۳۹



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 شیء بنیاد توسط جبر پردازش ای"

در تاریخ ۱۳۸۶/۰۸/۲۳ نمره نهایی پایان نامه: ۱۹,۸ به عدد نوزده و هشتادم به حروف
و درجه ۱ ارزیابی نمود.

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

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



دانشگاه تهران

پردیس دانشکده‌های فنی

دانشکده مهندسی برق و کامپیوتر

عنوان:

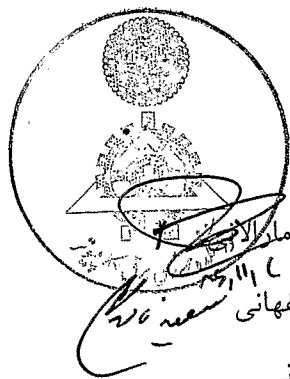
درستی‌یابی صوری سیستم‌های شیء‌بنیاد توسط جبر پردازش‌های

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.



دکتر جواد فیض

معاونت آموزشی تحصیلات تکمیلی پردیس دانشکده‌های فنی:

دکتر پرویز جبه‌دار

رییس دانشکده مهندسی برق و کامپیوتر:

دکتر سعید نادر اصفهانی

معاونت پژوهشی و تحصیلات تکمیلی دانشکده:

دکتر مرجان سیرجانی

استاد راهنما:

دکتر ناصر یزدانی

استاد مشاور:

دکتر فتنه تقی‌یاره

عضو هیأت داوران:

دکتر رامتین خسروی

عضو هیأت داوران:

دکتر سید حسن میریان حسین‌آبادی

عضو هیأت داوران:

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 پایان‌نامه 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:

تقديم به ساحت مقدس يوسف 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 کسب 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 بزرگووارم 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. با وجود 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 جبرپدازه‌ای استفاده می‌کنیم، که رویکردی قدرتمند برای مدل‌سازی سیستم‌های همروند است. با فراهم کردن نگاشتی از زبان‌های مبتنی بر شیء به جبرپدازه‌ای، می‌توانیم از توانمندی‌های جبرپدازه‌ای در کاربردهای صنعتی نیز استفاده کنیم. در نگاشت ارائه شده به طور خاص بر جبرپدازه‌ای $mCRL2$ تمرکز می‌کنیم، که یک شکل از جبرهای پدازه‌ای 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 ریکاست، 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 جبرپدازه‌ای، 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 ریکا 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 کندتر 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
۱.....مقدمه:	۱
۷.....دست‌آوردهای پایان‌نامه	۱-۱
۸.....زبان مبتنی بر شیء	۲-۱
۹.....ساختار پایان‌نامه	۳-۱
۱۰.....کارهای مشابه:	۲
۱۸.....زبان‌های تبدیل‌شده به mCRL2	۱-۲
۱۹.....پیش‌زمینه‌ها:	۳
۲۰.....سیستم‌های گذار: مبتنی بر حالت و مبتنی بر کنش	۱-۳
۲۱.....کنش‌های پنهان راکد	۱-۱-۳
۲۳.....منطق‌های زمانی	۲-۳
۲۵.....هم‌ارزی رفتارها	۳-۳
۲۷.....دوشبیه‌سازی	۱-۳-۳
۲۸.....دوشبیه‌سازی قوی	۱-۱-۳-۳
۳۰.....دوشبیه‌سازی ضعیف	۲-۱-۳-۳
۳۱.....دوشبیه‌سازی انشعابی	۳-۱-۳-۳
۳۲.....هم‌ارزی لکتی	۲-۳-۳
۳۴.....جمع‌بندی	۳-۳-۳
۳۵.....جبرپروندهای mCRL2:	۴
۳۶.....مقدمه‌ای بر جبرپروندهای	۱-۴
۳۹.....خرد زبان نمایش مشترک (μ CRL)	۲-۴

۳۹	فلسفه‌ی ایجاد	۱-۲-۴
۴۱	انواع داده‌ای مجرد	۲-۲-۴
۴۶	مقدمه‌ای بر μ CRL	۳-۲-۴
۴۷	ترکیب‌گزینی و متوالی	۱-۳-۲-۴
۵۰	پردازه‌های موازی	۲-۳-۲-۴
۵۲	بن‌بست و بسته‌بندی	۳-۳-۲-۴
۵۳	اعلان‌پردازه‌ها	۴-۳-۲-۴
۵۴	عبارات شرطی	۵-۳-۲-۴
۵۵	جمع‌زنی بر روی یک نوع داده‌ای	۶-۳-۲-۴
۵۶	تغییر نام	۷-۳-۲-۴
۵۷	پنهان‌سازی کنش‌ها	۸-۳-۲-۴
۵۸	توسعه‌های mCRL2 نسبت به μ CRL	۳-۴
۵۹	انواع داده‌ای جدید در mCRL2	۱-۱-۳-۴
۶۰	چندکنش‌ها	۲-۱-۳-۴
۶۴	نگاشت ربکا (سریر):	۵
۶۶	زبان ربکا	۱-۵
۶۷	طرح‌نگاشت	۲-۵
۷۳	پیاده‌سازی و مطالعات موردی	۳-۵
۷۶	بررسی کاهش فضای حالت	۴-۵
۷۹	خلاصه‌ی فصل	۵-۵
۸۰	نگاشت SystemC:	۶
۸۱	مقدمه	۱-۶
۸۴	زبان SystemC	۲-۶
۸۷	انواع داده‌ای هسته	۳-۶

۹۰.....	پردازه‌های هسته.....	۴-۶
۹۲.....	از پردازه‌های SystemC به پردازه‌های mCRL2.....	۵-۶
۹۳.....	وراسی کد.....	۶-۶
۹۴.....	مطالعه‌ی کاربردی.....	۷-۶
۹۵.....	خلاصه فصل.....	۸-۶
۹۷.....	الگوریتم‌های کاهش:	۷
۹۹.....	سرآغازی بر روش‌های کاهش فضای حالت.....	۱-۷
۱۰۱.....	خطی‌سازی.....	۲-۷
۱۰۳.....	کاهش ترتیب جزئی.....	۳-۷
۱۰۵.....	ت-همریزی و ت-اولویت‌دهی.....	۱-۳-۷
۱۰۸.....	کاهش ترتیب جزئی در ساختارهای کریپکه.....	۲-۳-۷
۱۱۲.....	روش پیاده‌سازی.....	۱-۲-۳-۷
۱۱۶.....	کافی بودن کاهش ترتیب جزئی.....	۳-۳-۷
۱۱۶.....	مخروط‌ها و کانون‌ها.....	۴-۷
۱۱۹.....	نتیجه‌گیری و کارهای آینده:	۸
۱۲۳.....	ضمیمه:	۹
۱۳۲.....	فهرست منابع.....	
۱۳۸.....	فرهنگ واژگان (انگلیسی به فارسی).....	
۱۴۳.....	فرهنگ واژگان (فارسی به انگلیسی).....	

فهرست شکل‌ها

عنوان.....	صفحه
شکل ۱-۲: ترجمه‌ی $X - (Y + 1)$	۱۳
شکل ۲-۲: چارچوبی برای زبان‌های شیء‌گرا در CCS.....	۱۴
شکل ۱-۳: کنش داخلی قابل رؤیت نیست.....	۲۲
شکل ۲-۳: کنش داخلی به طور غیرمستقیم قابل رؤیت است.....	۲۳
شکل ۳-۳: طیف فان‌خلاییک.....	۲۶
شکل ۴-۳: یک رابطه‌ی دوشبیه‌سازی که متعددی نیست.....	۲۸
شکل ۵-۳: دو رابطه‌ی دومشابه.....	۲۹
شکل ۶-۳: دو پردازهی دومشابه ضعیف.....	۳۱
شکل ۷-۳: دو مسیر هم‌ارز لکتی.....	۳۳
شکل ۱-۴: شبه‌کد دفترچه تلفن در روش مبتنی بر مدل (برگرفته از (Jackson 2006)).....	۴۲
شکل ۲-۴: شبه‌کد دفترچه تلفن در روش جبری (برگرفته از (Jackson 2006)).....	۴۲
شکل ۳-۴: انجام یک گذار.....	۴۶
شکل ۴-۴: سه پردازهی متوالی.....	۴۷
شکل ۵-۴: دو پردازهی استفاده از انتخاب.....	۴۸
شکل ۶-۴: عدم پخشی ترکیب متوالی بر ترکیب‌گزینی از سمت چپ.....	۴۹
شکل ۷-۴: توصیف یک ساعت در μCRL	۵۴
شکل ۸-۴: یک شبکه‌ی پتری ساده.....	۶۱
شکل ۱-۵: یک مدل ساده برای ربکا.....	۶۶
شکل ۲-۵: نمودار تبادل پیغام در مدل $mCRL2$	۶۸
شکل ۳-۵: ترجمه‌ی مدل ربکای شکل ۱-۵ به $mCRL2$	۷۰
شکل ۴-۵: یک نمونه کد ربکا برای تولیدکننده-مصرف‌کننده.....	۷۶
شکل ۵-۵: فضای حالت شکل ۴-۵.....	۷۷
شکل ۶-۵: اضافه کردن کنش مصنوعی sel	۷۸

- شکل ۱-۶: یک پیمانانه به زبان SystemC برای DFF ۸۵
- شکل ۲-۶: انواع داده‌ای که در کد mCRL2 استفاده می‌شوند ۸۹
- شکل ۳-۶: پردازش‌های هسته در mCRL2 ۹۰
- شکل ۴-۶: ترجمه‌ی پردازش‌های شکل ۱-۶ ۹۳
- شکل ۵-۶: پردازش‌ی درستی‌یاب برای شکل ۱-۶ ۹۴
- شکل ۱-۷ (الف): سه گذار همروند ب) تمام در همسازیه‌ی ممکن پ) یک روند اجرا ۱۰۴
- شکل ۲-۷: الگوی همریزی ۱۰۵
- شکل ۳-۷: مثال برای همریزی. در (الف) همه‌ی گذارهای τ جزء مجموعه‌ی τ -همریز حداکثرند، در (ب) هیچ کدام ۱۰۶
- شکل ۴-۷: استفاده از τ -اولویت‌دهی ۱۰۷
- شکل ۵-۷: دو گذار مستقل ۱۰۹
- شکل ۶-۷: جایگزین کردن گذارها بر مبنای جابه‌جایی‌پذیری ۱۱۰
- شکل ۷-۷: یک مثال ساده به همراه فضای حالت کاهش یافته ۱۱۵
- شکل ۸-۷: یک کانون و مخروط آن ۱۱۷

فهرست جدول‌ها

عنوان.....	صفحه
جدول ۴-۱: اصول پایه برای μCRL	۴۸
جدول ۴-۲: اصول موضوعه برای موازات در μCRL	۵۱
جدول ۴-۳: اصول ناظر بر بن‌بست.....	۵۲
جدول ۴-۴: قواعد ناظر بر بسته‌بندی.....	۵۳
جدول ۴-۵: اصول ناظر بر عبارات شرطی.....	۵۴
جدول ۴-۶: اصول موضوعه‌ی عملگر جمع.....	۵۶
جدول ۴-۷: اصول موضوعه‌ی تغییر نام.....	۵۷
جدول ۴-۸: اصول موضوعه‌ی کنش پنهان در دوشبیه‌سازی انشعابی.....	۵۸
جدول ۴-۹: اصول موضوعه‌ی چندکنش‌ها.....	۶۲
جدول ۵-۱: نگاشت ربکا به $m\text{CRL}2$	۷۳
جدول ۵-۲: نگاشت ربکا به پروملا.....	۷۴
جدول ۵-۳: تعداد حالات و گذارهای واری‌مدل‌های ربکا در دو ابزار.....	۷۵

فصل اول

مقدمه

در حوزه‌ی دانش کامپیوتر، "روش‌های صوری"^۱ 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 بر این 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^۲ و واکنشی^۳ 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 لاند (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 سیستم عامل 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^۴ و نظائر آن را در نظر داشته باشد. بسته به پارامترهای رفتار/سیستم، درهم‌سازی^۵ / درهم‌سازی، خطی / انشعابی بودن زمان، مدل‌های متفاوتی را می‌توان برای یک سیستم همروند در نظر گرفت (Sassone, Nielsen et al. 1996).

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

¹ Formal Methods

² Sequential

³ Reactive

⁴ Starvation

⁵ Interleaving

جبری به پردازش‌های موازی در دهه‌ی هفتاد با معرفی "پردازش‌های ترتیبی مرتبط"^۱ توسط تونی هر^۲ (Hoare 1978; Hoare 1985) و نیز "حساب سیستم‌های مرتبط"^۳ توسط رابین میلنر^۴ (Milner 1980; Milner 1989) آغاز شد. برای اولین بار یان برخسترا^۵ و یان ویلم کلاپ^۶ در "جبر پردازش‌های مرتبط"^۷ به این شیوه از مدل‌سازی سیستم‌های همروند نام "جبر پردازش‌ای" دادند (Bergstra and Klop 1984; Baeten and Weijland 1990)، که تا امروز نیز به کار برده می‌شود. سه جبر پردازش‌ای نامبرده در فوق، اصلی‌ترین رویکردهای موجود هستند و باقی جبر پردازش‌ها معمولاً در موارد خاص به کار گرفته می‌شوند، مثل حساب پای^۸ (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 پردازش‌ای CCS، CSP و ACP استفاده خواهیم نمود.

در نام هر سه جبر پردازش‌ای نامبرده، بر روی ارتباط تأکید شده است. علت این نام‌گذاری از آنجا ناشی می‌شود که در جبر پردازش‌ای، هدف توصیف و استدلال در زمینه‌ی سیستم‌های مرتبط است. چنین سیستم‌هایی از طریق یک سری ارتباطات با جهان اطراف خود کنش دارند. در جبر پردازش‌ای از محاسبات داخلی درونی هر پردازش (متغیرها، تخصیص دادن مقدار به متغیر،...) کلاً صرف نظر می‌شود. به عبارت دیگر یک دید سطح بالا به سیستم وجود دارد، که تمامی سیستم‌های مرتبط را به صورت مجرد پردازش می‌بیند، به طوری که هر پردازش عضوی از یک دامنه‌ی ریاضی است. پردازش‌ها توسط یک سری عملگر قابل ترکیبند. برای مثال، عملگرهایی برای ترکیب ترتیبی و یا موازی پردازش‌ها وجود دارند. قواعدی نیز در هر جبر پردازش‌ای 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 پردازش‌ای شامل یک دامنه از پردازش‌ها 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 پردازها دید مجرد ندارند. به عنوان مثال در این زمینه، می‌توان به شبکه‌های پتری (Murata 1989) اشاره کرد. شبکه‌های پتری، پردازها را جزئی‌تر و عینی‌تر از جبر پردازها توصیف می‌کنند (Olderog 1991)؛ حال آنکه در جبر پردازهای پردازها موجوداتی مجردند و تأکید بر نحوه ترکیب آنهاست. در شبکه‌های پتری، رابطه‌های علی 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 دلایل 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^۱ 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^۲ محاسبات درونی پنهان می‌شوند، به طوری که تنها ارتباط ورودی/خروجی از پیاده‌سازی باقی بماند. در نهایت، عبارت پردازهای باقی‌مانده توسط منطق برابری^۳ 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 پردازهای $Spec$ 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 در آن منظور از تساوی، یک شکل از هم‌ارزی^۱ در جبر پردازش‌های مثل "دوشباهت انشعابی"^۲ است. در این فصل تنها یک شمای کلی از درستی‌یابی در جبر پردازش‌های مورد تأکید است، و نمادهای استفاده شده در رابطه‌ی فوق در فصل‌های بعدی شرح داده شده‌اند.

توسط اصول موضوعی^۳ جبرهای پردازش‌های، 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^۴ 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^۵ یک شمارنده بایستی قرار داده شود. اما در توصیف رفتار پروتکل (سمت راست رابطه‌ی درستی‌یابی جبر پردازش‌های)، 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 پردازش‌های 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 پردازش‌های یافتن پاسخ به این سؤال بود که آیا می‌توان جبر پردازش‌های را برای مسائل جدی‌تر و بزرگ‌تر استفاده کرد یا خیر. مقداری از این چالش در جبر پردازش‌های لوتوس^۶ (Tommaso and Ed 1987) پاسخ داده شده است. در لوتوس انواع داده‌ای و مقداری "شکر نحوی" به زبان اضافه شده‌اند. جبر پردازش‌های دیگری که سعی در حل موضوع دارد، μ CRL (Groote and

¹ Equivalence

² Branching bisimilarity

³ Axioms

⁴ Alternating bit protocol

⁵ Time-out

⁶ LOTOS

(Ponse 1994) است. μ CRL نسبت به لوتوس ساده‌تر است، به طوریکه تنها با دو عملگر if-then-else و جمع در دامنه‌های نامتناهی انواع داده‌ای را به جبر پردازش‌های 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 پردازش‌های μ CRL و خصوصاً روایت جدید آن، mCRL2 (Groote, Mathijssen et al. 2005) است. مزیت mCRL2 نسبت به جبرهای پردازش‌های که سابقاً در این زمینه به کار گرفته شده‌اند در موارد زیر قابل خلاصه کردن است:

۱. وجود الگوریتم‌ها و تکنیک‌های قدرتمند کاهش. جبرپردازش‌های 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 جبرپردازش‌های، استفاده کردن از این روش‌ها بوده است.

۲. مناسب بودن زبان برای ترجمه. نام جبرپردازش‌های mCRL2 (micro Common Representation Language 2 یا خرد زبان نمایش مشترک 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 جبرپردازش‌های اثبات کردن درستی سیستم توسط اصول موضوعه‌ی جبرپردازش‌های است. اما با بزرگ شدن سیستم‌ها و دشوار شدن توصیف آنها، سروکار داشتن مستقیم با روابط مشخص‌کننده‌ی آنها کاری سخت و دشوار است. برای این منظور، یک ابزار پشتیبان برای این جبرپردازش‌های 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.