بسم الله الرحمن الرحیم

دفتر صحافی مبارک

تبریز: فلکه دانشگاه پاساژ نسیم، زیرزمین پلاک ۲۶ تلفن: ۳۳۶۴۶۸۰

۰۹۱۴۳۱۳۰۰۴۹ - ۰۹۱۴۱۱۵۰۰۴۹

دانشکده‌ی علوم ریاضی
گروه ریاضی کاربردی

رساله
برای دریافت درجه دکتری در رشته‌ی
ریاضی کاربردی، گرایش سیستم‌های کامپیوتری

عنوان

یک روش صوری برای توصیف و درستی‌یابی ترکیبی سیستم‌های نرم‌افزاری مبتنی بر مولفه‌ها

استاد راهنما
دکتر آیاز عیسی‌زاده

اساتید مشاور
دکتر سید حسن میریان
دکتر میرکمال میرنیا

پژوهشگر
جابر کریمپور ینگجه

زمستان ۱۳۸۷

بِسمِ اللّهِ الرّحمنِ الرّحیم

حمد وسپاس بی‌قیاس ذات پاک خدایی را سزد که سخنوران در ستودن او بمانند، شمارگران شمردن نعمت‌های او ندانند و کوشندگان حق او را گزاردن نتوانند. خدایی که پای اندیشه تیزگام در راه شناسایی او لنگ است، و سر فکرت ژرف رو به دریای معرفتش بر سنگ. صفت‌های او تعریف نشدنی، به وصف در نیامدنی، در وقت ناگنجیدنی و به زمان مخصوص نابودنی است. به قدرتش عالم و عالمیان را وجود بخشید و برای هدایت آنها پیامبران را بر انگیخت.

از فرمایشات حضرت علی(ع)

اکنون که باعنایت و الطاف بیکران الهی و با بهره‌مندی از نعمت‌های بیشمار او دوره‌ی دکترای ریاضی کاربردی با گرایش سیستم‌های کامپیوتری را به پایان رسانیده و مسئولیت خطیر معلم بودن را پذیرا می‌شوم از ذات مقدسش مدد می‌جویم تا در انجام این وظیفه حساس لحظه‌ای کوتاهی ننمایم. قداست و معنویت تعلیم و تعلم را در توسعه علم و فن‌آوری با حفظ ارزش‌های الهی مدنظر داشته باشم و از آلودن آن به اغراض مادی، هواهای نفسانی و وسوسه‌های شیطانی اجتناب نمایم.

بار الها، ترا به خاطر این نعمت عظیم شاکرم که با فارغ التحصیلی اینجانب، پسر عزیزم پویا به مدرسه می‌رود و صندلی من در کلاس درس خالی نمی‌ماند.

و لَمْ یَشْکُر الْمَخلوق لَمْ یَشْکُر الْخالِقْ.

در طول دوران تحصیلاتم اساتید بسیاری بوده‌اند که هر یک نقش بسزایی در پیشرفت اینجانب داشته‌اند. در این میان اساتیدی نیز هستند که همچون ستاره‌ای تابناک در آسمان علم و دانش و انسانیت درخشیده‌اند و گوشه‌ای از تاریکی جهل مرا به نور علم خود مزین کرده‌اند. می‌دانم که هیچ کلمه‌ای را یارای آن نیست که گوشه‌ای از زحمات استاد گرانقدرم جناب آقای دکتر آیاز عیسی‌زاده را که بارها و بارها از نظر علمی و همینطور روحی و روانی پشتیبان من بوده‌اند، جبران نماید. همچنین، می‌دانم که تاپایان عمر خود نخواهم توانست ذره‌ای از محبت‌های استاد عزیزم جناب آقای دکتر میرنیا را جبران کنم. تنها کاری که در حال حاضر می‌توانم انجام دهم آن است که از درگاه صمدیت و بارگاه عبودیت به این دو استاد بزرگوار آرزوی سلامتی و سر بلندی بخواهم و بگویم سپاسگزارم.

بر خود لازم می‌دانم از استاد مشاور ارجمندم جناب آقای دکتر سید حسن میریان از دانشکده‌ی مهندسی کامپیوتر دانشگاه صنعتی شریف که در دوران تحصیلی دکترای اینجانب، زحمات زیادی را متحمل شده‌اند و با توصیه‌های مفید خود، مرا در انجام تحقیقات و تدوین این رساله یاری نموده‌اند، تشکر نمایم.

همچنین از ریاست محترم دانشکده‌ی علوم ریاضی جناب آقای دکتر امامعلی پور، آقایان دکتر جباری، دکتر خیری، دکتر شهمراد، دکتر مهری و دوستان ارجمندم (احمد، مرتضی، جعفر، قدرت، اصغر، رمضان و ...) تشکر می‌کنم.

بار دیگر از ابتکار حکیمانه استاد عزیز آقای دکتر میرنیا و از مساعدت استاد ارجمند آقای دکتر رحیمی در ایجاد دکترای ریاضی کاربردی با گرایش سیستم‌های کامپیوتری، تشکر و قدردانی می‌نمایم.

از داوران محترم خارج از دانشگاه تبریز آقایان پروفسور محمدرضا میبدی از دانشگاه صنعتی امیر کبیر و پروفسور علی موقر از دانشگاه صنعتی شریف که با قبول زحمت و صرف وقت، این رساله را داوری فرمودند و با حضور در شهر تبریز و جلسه دفاعیه اینجانب موجب ترغیب اینجانب به مطالعه و تحقیق هرچه بیشتر شدند؛ صمیمانه تشکر و قدردانی می‌نمایم. همچنین از استاد محترم دانشکده‌ی علوم ریاضی جناب آقای دکتر سعید صالحی که داوری این رساله را تقبل فرمودند تشکر می‌کنم.

در پایان از همسر عزیزم خانم مهندس آبادی که در تمامی مراحل همواره یار و مشوق من بوده‌اند، سپاسگزارم. از خداوند متعال برای پسر عزیزم پویا — که در دوران کودکی او همواره به درس و تدوین این رساله مشغول بوده‌ام — آرزوی سلامتی، درجات والای انسانی و علمی دارم.

جابر کریم‌پور

نام خانوادگی دانشجو: کریم پور ینگجه نام: جابر

عنوان: یک روش صوری برای توصیف و درستی‌یابی ترکیبی سیستم‌های نرم‌افزاری مبتنی بر مولفه‌ها

استاد راهنما: دکتر آیاز عیسی‌زاده

اساتید مشاور: دکتر سید حسن میریان ، دکتر میرکمال میرنیا

مقطع تحصیلی: دکتری رشته: ریاضی کاربردی گرایش: سیستم‌های کامپیوتری دانشگاه تبریز

دانشکده علوم ریاضی تاریخ فارغ‌التحصیلی: زمستان ۱۳۸۷ تعداد صفحه: ۱۳۷

کلید واژه‌ها: درستی‌یابی ترکیبی، خودکار واسط، کنترل کننده، گره، مولفه، ویوچارت

چکیده

با توجه به اهمّیّت توصیف سیستم‌های نرم‌افزاری با استفاده از روش‌های ریاضی، در این رساله یک مدل ریاضی برای توصیف سیستم‌های تشکیل شده از مولفه‌ها، ارائه می‌کنیم؛ به این ترتیب که برای هر مولفه با رخدادهای گسسته، یک مدل ریاضی درنظر گرفته و پروتکل ارتباطی آن مولفه با سایر مولفه‌ها را با استفاده از خودکارهای واسط، تعریف می‌کنیم. همچنین در کنار مولفه‌های اوّلیه، یک مدل ریاضی دیگری بنام گره ارائه می‌کنیم که برای توصیف و طراحی سلسله مراتبی سیستم‌ها به کار می‌رود. یک گره ساختار درختی دارد و از مجموعه زیرگره‌ها تشکیل شده‌است. هر زیرگره به نوبت خود، یک گره و یا یک مولفه است که تحت کنترل یک مدل ارائه شده‌ی دیگری بنام کنترل کننده، کار می‌کند. به این ترتیب، گره توصیف کننده‌ی کل سیستم عنوان ریشه‌ی درخت و مولفه‌های اولّیه، برگ‌های درخت را تشکیل می‌دهند. کنترل کننده نیز همانند گره، ساختار سلسله مراتبی دارد و برگ‌های آن، خودکارهای واسط می‌باشند. این مدل

ریاضی، پروتکل ارتباطی میان گره‌ها را توصیف می‌کند. این پروتکل نه تنها شامل چگونگی پاسخ گره نسبت به ورودی‌ها است؛ بلکه شامل فرضیات محیطی است که از این گره استفاده خواهد کرد. از طرفی این پروتکل، جزئیات پیاده‌سازی داخل گره‌ها و مقادیر داده‌های منتقل شده بین آنها را شامل نمی‌شود. در نتیجه، اولاً؛ به دلیل خلاصه بودن کنترل کننده‌ها نسبت به گره‌ها، فضای حالت آنها نسبت به گره‌ها از تقلیل قابل توجهی برخوردار است و ثابت خواهیم کرد که بسیاری از ویژگی‌های سیستم را با استفاده از کنترل کننده‌ها می‌توانیم وارسی کنیم. ثانیاً؛ امکان توسعه‌ی مستقل گره‌ها (مولفه‌ها) و استفاده مجدد از آنها فراهم می‌شود. ثالثاً؛ امکاناتی برای تحلیل و درستی‌یابی ترکیبی سیستم نهایی فراهم می‌شود.

از طرفی برای توصیف رفتار زیرسیستم‌های یک سیستم بزرگ و ناهمگن، می‌شود از زبان‌های مختلفی استفاده کرد. در میان زبان‌های متعدد، زبان‌های گرافیکی با معانی رسمی، اهمیّت بسزایی دارند. ما در این رساله، با توجه به معانی عملیاتی مولفه‌ها و گره‌ها، یک چارچوب اساسی برای توصیف و درستی‌یابی سیستم‌های مبتنی بر مولفه‌ها ارائه می‌کنیم که در آن هر مولفه با یک زبان گرافیکی مانند ویوچارت مدلسازی شده باشد. برای این کار، مستقیما مولفه‌ی توصیف شده با ویوچارت را به گره تبدیل نمی‌کنیم؛ در عوض، مفسّری طراحی می‌کنیم که با توجه به معنی زبان مدلسازی گرافیکی (ویوچارت)، معنای یک مولفه را برحسب حالت‌های قابل رسیدن و انتقالات آن در محیط داده شده، تعریف می‌کند. در نهایت و با استفاده از این مفسّر، یک ابزار کامپیوتری طراحی می‌کنیم که فضای حالت مورد نیاز یک گره را ساخته و به کمک روش وارسی ترکیبی گره، ویژگی‌های دلخواه آن را وارسی می‌کند. ملاحظه خواهیم کرد که روند محاسبه‌ی حالت‌های قابل رسیدن و انتقالات یک مولفه، اغلب مستقل از یک زبان خاص مانند ویوچارت است و برای تمام زبان‌های گرافیکی قابل استفاده می‌باشد.

فهرست مطالب

لیست اشکال

پیشگفتار

در چند سال گذشته، تکنیک مهندسی نرم‌افزار مبتنی بر مولفه‌ها، برای توسعه‌ی نرم‌افزارهایی با مقیاس بزرگ و پیچیده، مفید واقع شده است؛ زیرا با ساختن سیستم‌ها از مولفه‌های توسعه یافته‌ی مجزا، امکان استفاده‌ی مجدد، توسعه‌ی سریع و امکان مدیریت پیچیدگی فراهم می‌شود. کشف و حذف خطاها در مراحل اولیّه تحلیل و طراحی سیستم‌های مبتنی بر مولفه‌ها، یک امر مهمّ حیاتی و اقتصادی است و تصحیح آنها در قدم‌های بعدی توسعه، سخت و گران قیمت خواهد بود؛ زیرا طراحی و پیاده‌سازی نیازمندی‌های غیر صحیح موجب شکست نرم‌افزار و حتی ممکن است موجب خسارات فراوان جانی و مالی شود[۸۴]. برای پیشگیری از اینگونه حوادث، در توصیف و طراحی سیستم‌های رایانه‌ای از روش‌های قابل اعتماد و مبتنی بر ریاضیات، استفاده می‌کنند؛ زیرا توصیفات منطقی و غیر مبهم از رفتار یک سیستم، در کشف ابهامات و ناسازگاری‌ها کمک شایانی می‌کند و امکان توسعه‌ی درست آن را تا حدودی فراهم می‌نماید. تحقیقات نشان می‌دهد که در مهندسی نرم‌افزار مبتنی بر مولفه‌ها، با زیاد شدن تعداد مولفه‌های متعامل، تحلیل کل سیستم با محدودیت‌های حافظه و پیچیدگی الگوریتم‌ها روبرو شده و این امر موجب افزایش نمائی تعداد خطاهای سیستم می‌گردد[۵].

برای درستی‌یابی خودکار سیستم‌های همروندی با تعداد حالات متناهی، از روش **وارسی الگو**[۱]، استفاده می‌شود[۱۵]. در این روش، ابتدا فضای حالت[۲] یک سیستم که نمایشی از تمامی حالت‌ها و انتقالات بین آنها است، ساخته می‌شود. روند وارسی، جستجوی کل فضای حالت سیستم برای این منظور است که آیا ویژگی‌های مورد نظر در فضای حالت برآورده می‌شود یا نه؟عیب اوّل این روش، انفجار تعداد حالت‌ها در ساخت فضای حالت سیستم‌های بزرگ است. عیب دوّم روش **وارسی الگو** این است که در این روش، لازم است تمامی سیستم با یک زبان مدلسازی شود؛ در حالی که بهتر است برای مدلسازی جنبه‌های مختلف سیستم‌های بزرگ، از زبان‌های مختلف استفاده شود.

به دلیل محدودیت بالا در روش‌های وارسی متداول، بحث درستی‌یابی ترکیبی این سیستم‌ها با

---

[۱] Model Checking

[۲] State Space

استفاده ازتکنیک تقسیم وحل، مطرح شده است[۲۹]. در درستی‌یابی ترکیبی، برای جلوگیری از انفجار تعداد حالت‌ها در فضای حالت، تک تک مولفه‌ها را به صورت جداگانه وارسی کرده و از درستی آنها، درستی کل سیستم را نتیجه می‌گیرند[۳۰، ۱۰۰]. اما بدلیل کمبود اطلاعات از محیط مورد استفاده‌ی مولفه‌ها و وابستگی شدید آنها به محیط، درستی‌یابی ترکیبی چندان موفق نبوده و یا در مواردی به صورت غیر رسمی انجام می‌گیرد. لذا ارائه‌ی یک روش صوری برای مدل‌سازی و درستی‌یابی سیستم‌های مبتنی بر مولفه‌هاضروری به نظر می‌رسد.

برای رسیدن به این هدف، در این رساله یک مدل ریاضی برای مدلسازی رفتار سیستم‌های تشکیل شده از مولفه‌ها، ارائه می‌کنیم؛ به این ترتیب که برای هر مولفه‌ی اوّلیه با رخدادهای گسسته و اولویت دار[۳] (DECsP)، یک مدل ریاضی درنظر گرفته و پروتکل ارتباطی آن مولفه با سایر مولفه‌ها را با استفاده از خودکارهای واسط (IAs)[۴]، تعریف می‌کنیم. این خودکارها، روشی برای توصیف واسط مولفه‌های نرم‌افزار ارائه کرده و طراحی مولفه‌ها را تحت فرضیات محیط در نظر می‌گیرند. یک خودکار واسط تنها رفتارهایی را قبول می‌کند که به وسیله محیط تولید می‌شوند و برای خودکار قانونی هستند. با قبول نکردن بعضی از ورودی‌ها، این فرضیه بیان می‌شود که محیط نباید چنین ورودی‌ها را تولید کند.

همچنین در این رساله، برای توصیف و طراحی رفتار سلسله مراتبی سیستم‌ها، در کنار مولفه‌های اوّلیه، مدل ریاضی دیگری بنام گره[۵] ارائه می‌کنیم. یک گره ساختار درختی دارد و از مجموعه زیرگره‌ها تشکیل شده است که هر زیرگره به نوبه‌ی خودش یک گره و یا یک مولفه است که تحت کنترل یک مدل ارائه شده دیگری بنام کنترل کننده کار می‌کند. به این ترتیب که گره ریشه، توصیف کننده‌ی کل سیستم است و مولفه‌های اولّیه، برگ‌های درخت را تشکیل می‌دهند. کنترل کننده نیز همانند گره، ساختار سلسله مراتبی دارد و برگ‌های آن، خودکارهای واسط می‌باشند. مدل ریاضی کنترل کننده، پروتکل ارتباطی میان گره‌ها را توصیف می‌کند. این پروتکل نه تنها شامل چگونگی پاسخ گره نسبت به ورودی‌ها است بلکه شامل فرضیات محیطی است که از این گره استفاده خواهد کرد. ثابت خواهیم کرد که بسیاری از

[۳] Discrete Event Components with Priority

[۴] Interface Automata

[۵] Node

ویژگی‌های گره‌ها را از طریق وارسی کنترل کننده‌ها می‌توانیم درستی‌یابی کنیم. چون کنترل کننده‌ها جزئیات پیاده‌سازی داخل گره‌ها و مقادیر داده‌های منتقل شده بین آنها را شامل نمی‌شوند؛ لذا، به دلیل خلاصه شدن سیستم از گره‌ها به کنترل کننده‌ها، تقلیل قابل توجهی در فضای حالت سیستم رخ می‌دهد.

در قسمت دیگری از این رساله، با در نظر گرفتن معانی عملیاتی مولفه‌ها و گره‌ها، یک چارچوب اساسی را برای تهیه‌ی سیستم‌های مبتنی بر مولفه‌ها ارائه می‌کنیم که در آن هر مولفه با یک زبان گرافیکی مدل‌سازی شده باشد. با توجه به مزایای **ویوچارت**[۶] نسبت به سایر زبان‌ها و از طرفی جهت توسعه‌ی رساله‌ی دکترای عیسی‌زاده[۴۳]، ما این زبان را برای توصیف مولفه‌ها انتخاب کرده‌ایم. با داشتن مولفه‌ها، در دو مرحله زیر معنای عملیاتی یک مولفه‌ی توصیف شده با **ویوچارت** را تعریف می‌کنیم:

- **طراحی مفسّر:** در این مرحله، با توجه به معنی **ویوچارت**، اطلاعاتی را در مورد حالت‌ها و انتقالات مولفه‌ها بدست آورده و به صورت خودکار بررسی می‌کنیم که چگونه و چه انتقالات شدنی یا قدم‌هایی را یک مولفه در یک حالت یا ویوی مشخّص در ویوچارت برمی‌دارد. برای تعریف مفسّر معنایی به ویوچارت از خودکارهای نگاشت اشیاء(OMA)[۷]، استفاده خواهیم کرد[۵۹].

- **طراحی ابزار تحلیل**[۸]: در این مرحله، به صورت مستقل از ویوچارت و به استناد نتایج مرحله‌ی اوّل، حالت‌های قابل رسیدن را محاسبه کرده و با در نظر گرفتن فرضیات محیط مورد استفاده‌ی مولفه‌ها، فضای حالت سیستم ساخته می‌شود. برای این منظور ابزاری را طراحی می‌کنیم که معنای عملیاتی مولفه‌ها را برحسب DECs و در نهایت برحسب گره‌ها تعریف کند.

برای توسعه‌ی مستقل این دو قدم، قراردادی را وضع می‌کنیم که رفتار متقابل مفسّر و ابزار را بطور صریح تعریف می‌کند. به این ترتیب معنای یک مولفه در محیط داده‌شده را برحسب حالت‌های قابل رسیدن و انتقالات آن، تعریف می‌کنیم. ملاحظه خواهیم کرد که روند محاسبه‌ی حالت‌های قابل رسیدن و انتقالات یک مولفه، اغلب مستقل از ویوچارت است و برای تمام زبان‌ها قابل استفاده می‌باشد.

---

[۶] Viewcharts

[۷] Object Mapping Automata

[۸] Analysis Tools

فصل ۱

مقدمه

با پیشرفت سریع فنّاوری اطلاعات، سیستم‌های رایانه‌ای مورد استفاده در زندگی انسان‌ها روز به روز بزرگتر و پیچیده‌تر می‌شوند. در حالت کلی، اعمال توصیف، ساخت، مدیریت، فهم و نگهداری سیستم‌های نرم‌افزاری با مقیاس بزرگ آسان نیست. در اواخر قرن گذشته، روش‌های مقابله با بزرگی این سیستم‌ها، جداکردن توصیفات ساختاری از توصیفات رفتاری آنها بود که در نتیجه زبان‌های پیکربندی[۱] در زمینه‌ی توصیف ساختار سیستم‌ها و روش‌های صوری مانند Z [۱۰۱]، LOTOS [۶۹] و Statecharts [۳۷، ۳۸] در باب توصیف رفتار سیستم‌ها مطرح شدند. در اوایل این دهه، اندیشه‌ی تقسیم سیستم به مولفه‌ها و توسعه‌ی مستقل آنها مطرح شده و به دنبال آن، مهندسی نرم‌افزار مبتنی بر مولفه‌ها به عنوان یک راه‌حل برای توسعه‌ی نرم‌افزارهایی با مقیاس بزرگ و پیچیده پا به عرصه‌ی وجود گذاشت[۹۷].

تحقیقات انجام شده در زمینه‌های تولید مولفه‌ها، توصیف رفتار و تعامل بین آنها را می‌شود به دو گروه مختلف زبان‌های توصیف معماری[۲] (ADLs) مانند SOFA [۱۲]، Darwin[۷۵]، COSA[۶۶، ۹۴] و روش‌های کاملا صوری و بر اساس نظریه‌ی خودکارهای ورودی خروجی [۷۳، ۷۴]، مانند خودکارهای Team [۷۳، ۷۴]، خودکارهای تعامل [۸] و خودکارهای واسط [۱، ۲]، تقسیم‌بندی کرد. گروه اول برای توصیف ساختار مولفه‌ها، بیان ارتباطات و توصیف سلسله‌مراتبی از آنها، بسیار کار آمد هستند. ضعف این

---

[۱] Configuration Languages

[۲] Architecture Description Languages

زبان‌ها در توصیف ویژگی‌های متعامل و محدود بودن آنها در مساله‌ی درستی‌یابی است. اما خودکارهای گروه دوم، برخلاف زبان‌های ADL، کاملا صوری و کلی هستند و بطور گسترده توسط ابزارهای وارسی الگو پشتیبانی می‌شوند. با وجود این‌ها، این خودکارها صرفا برای مدل‌سازی تعامل در بین مولفه‌ها طراحی شده‌اند و برای طراحی ساختار مولفه‌ها و معماری سلسله‌مراتبی سیستم‌ها نامناسب‌اند. همچنین، در درستی‌یابی این خودکارها، مساله‌ی افزایش نمائی تعداد حالت‌ها در فضای حالت کل سیستم مشهود است.

در این رساله، یک روش مبتنی بر خودکارها ارائه می‌شود که از مزایای زبان‌های ADL برای توصیف معماری سلسله‌مراتبی سیستم‌ها و از زبان‌های مبتنی بر خودکارها، برای صوری کردن هرچه بیشتر و درستی‌یابی خودکار استفاده می‌کند. همچنین در این رساله، برای حل مسله‌ی افزایش تعداد حالت‌ها در فضای حالت کل سیستم، از روش درستی‌یابی ترکیبی استفاده می‌کنیم. هدف از درستی‌یابی ترکیبی[۳] این است که از اثبات درستی اجزای تشکیل دهنده یک سیستم، درستی کل آن سیستم را نتیجه بگیریم.

۱.۱ اصطلاحات

مولفه‌ی نرم‌افزار:[۴] واحدی برای شرکت در ترکیب است که دارای واسطهای به طور قراردادی توصیف شده و وابستگی‌های محیطی صریح و مشخص است. یک مولفه‌ی نرم‌افزار می‌تواند مستقلاً ایجاد و توسعه یابد و توسط شخص ثالثی در ترکیب استفاده شود[۹۸].

گره: [۵] یک مدل ریاضی با ساختار سلسله مراتبی است که از مجموعه زیرگره‌ها تشکیل می‌شود. هر زیرگره به نوبهٔ خود یک گره و یا یک مولفه است. به عبارتی از ترکیب چند مولفه، یک گره بوجود می‌آید.

پیکربندی یک گره: [۶] در مدل گسسته‌ی مولفه‌ها، یک مولفه در هر لحظه می‌تواند فقط در یک حالت باشد. اما وقتی سیستم را با گره نشان می‌دهیم؛ سیستم در یک لحظه می‌تواند در چندین حالت باشد؛ برای بیان فرق مفهوم حالتِ یک گره از حالتِ یک مولفه‌ی گسسته، به یک حالتِ گره، یک پیکربندی آن گره

---

[۳] Compositional Verification

[۴] Software Component

[۵] Node

[۶] Configuration of a Node

می‌گوییم.

خودکارهای واسط (IA):[۷] یک زبان صوری برای توصیف پروتکل ارتباطی میان مولفه‌های نرم افزار است که توسط آلفارو و هِنزنگر ارائه شده است[۱، ۲].

کنترل کننده: [۸] یک مدل ریاضی است که پروتکل ارتباطی میان گره‌ها را توصیف می‌کند. به عبارتی از ترکیب چند خودکار واسط، یک کنترل کننده بوجود می‌آید.

ویوچارت: یک زبان مدل‌سازی گرافیکی است که توسط عیسی‌زاده ارائه شده است[۴۳]. در این زبان، نیازمندی‌های رفتاری سیستم‌های بزرگ و پیچیده به صورت ترکیبی از دیدگاه‌های مختلف توصیف می‌شود. منظور از یک دیدگاه، یک توصیف کامل از رفتار یک سیستم از یک منظر مشخص است؛ به عنوان مثال، دید[۹] یک مشتری از یک کارگذار، رفتاری است که مشتری از کارگذار انتظار دارد.

۲.۱ بیان مسئله

مساله‌ی مورد بحث در این رساله، ارائه یک روش صوری برای توصیف و درستی‌یابی سیستم‌های مبتنی بر مولفه‌ها است. راه حل این مساله، انتخاب یک روش موجود و توسعه آن، یا ارائه یک روش جدید با ویژگی‌های زیر است:

۱) باید دقیق بوده، گرامر و معنای درست داشته باشد.

۲) باید برای ترکیب مولفه‌ها راه‌حل دلخواه ارائه کرده و توصیفی دقیق از پروتکل‌های ارتباطی مولفه‌ها را داشته باشد.

۳) باید امکان توصیف و طراحی جنبه‌های مختلف یک سیستم با زبان‌های مختلف را داشته باشد.

۴) باید توصیف و طراحی معماری سلسله مراتبی سیستم‌ها را فراهم نماید.

---

[۷] Interface Automata

[۸] Controller

[۹] View

۵) باید مشکل اساسی افزایش نمائی تعداد حالت‌ها در فضای حالت سیستم را حل کند و امکان تحلیل و درستی‌یابی کل سیستم را داشته بااشد.

٦) باید ضمن دقیق بودن از روش‌های صوری استفاده کند تا برای مهندسین نرم‌افزار قابل استفاده باشد.

۷) ابزاری برای مدلسازی، شبیه‌سازی و درستی‌یابی سیستم‌ها، داشته باشد.

روش صوری که ما دراین رساله ارائه می‌کنیم دارای شش ویژگی اوّل است. برای ویژگی هفتم، اصول اوّلیّه و الگوریتم‌های مربوطه را طراحی کرده و همچنین الگوهایی را برای ساخت ابزار مهندسی نرم‌افزار به کمک رایانه ارائه می‌کنیم. لازم به ذکر است که ما این الگوها را با استفاده از زبان برنامه‌سازی جاوا و کلاس‌های ارائه شده در مجموعه ابزارهای موزیز [۲٦]، پیاده‌سازی کرده‌ایم. این رساله، پیاده‌سازی یک ابزار کامل و مورد استفاده برای مهندسین نرم‌افزار را به عنوان کار پژوهشی آینده معرفی خواهد کرد.

۳.۱ اهداف

تدوین این رساله دو هدف زیر را دنبال می‌کند:

- مدل‌سازی صوری سیستم‌های مبتنی بر مولفه‌ها و توسعه‌ی تکنیک‌های درستی‌یابی با استفاده از تکنیک‌های موجود، برای درستی‌یابی ترکیبی این سیستم‌ها، بطوریکه از مشکل انفجار در فضای حالت جلوگیری شود. به عبارت دیگر، برای جلوگیری از انفجار فضای حالت در روش‌های معمولی وارسی الگو، در این رساله از روش درستی‌یابی ترکیبی استفاده می‌کنیم.
- با توجه به اینکه جنبه‌های مختلف یک سیستم بزرگ را نمی‌توان با یک زبان مدل‌سازی توصیف کرد، هدف دیگر ما، ایجاد امکانی برای توصیف زیرسیستم‌های مختلف سیستم‌های بزرگ، با استفاده از زبان‌های مدل‌سازی مختلف است بطوریکه امکان درستی‌یابی این سیستم‌های بزرگ نیز فراهم شود. چون در عمل از زبان‌های گرافیکی بطور گسترده استفاده می‌شود لذا در این رساله، به

این زبان‌ها می‌پردازیم. برای این منظور از میان زبان‌های گرافیکی، زبان ویوچارت را عملیاتی کرده و یک روش برای رسیدن به پیکربندی‌ها و انتقالات در ویوچارت ارائه می‌کنیم. ضمناً راه حل ارائه شده در این رساله، مخصوص ویوچارت نیست و برای تمامی زبان‌های گرافیکی مانند نمودارهای حالت[۱۰] [۳۷، ۳۸]، شبکه‌های پتری[۱۱] [۶۰]، نمودارهای همکاری UML [۸۲]، نمودارهای ترتیبی پیام‌ها MSCs [۶۸] و غیره قابل توسعه است. در نتیجه با داشتن روشی برای رسیدن به حالت‌ها و اجرای انتقالات در زیرسیستم‌های مختلف یک سیستم و با استفاده از مدل ارائه شده در هدف اوّل، امکان درستی‌یابی سیستم فراهم می‌شود.

۴.۱ نظریه

به نظر ما برای رسیدن به اهداف رساله و ارائه یک راه حل برای مساله‌ی مطرح شده در بخش ۲.۱، می‌توان کارهای زیر را انجام داد:

۱) تعریف یک نسخه‌ی توسعه یافته از مولفه‌های با رخدادهای گسسته به نام **مولفه با رخدادهای گسسته‌ی اولویت دار**[۱۲] (DECsP)، که در این نسخه، اولویت رخدادها نیز مدنظر قرار می‌گیرند.

۲) محصول موازی شده از سیستم‌های گذر حالت برای استفاده‌ی عملی مهندسین نرم‌افزار انتزاعی است و در بسیاری از سیستم‌ها کارائی چندانی ندارد. برای ارتباط بین مولفه‌ها و خودکارهای واسط، از بردارهای موازی سازی توسعه یافته استفاده می‌کنیم.

۳) برای ترکیب مولفه‌ها و مدل‌سازی سیستم‌های سلسله مراتبی، مدل ریاضی جدیدی بنام گره تعریف می‌کنیم. در داخل یک گره مجموعه زیرگره‌ها قرار می‌گیرند. زیرگره‌ها می‌توانند خودشان همانند یک گره رفتار کنند. به گره‌هایی که خودشان شامل زیرگره‌های دیگری نباشند، گره‌های پایه و یا

[۱۰] Statecharts

[۱۱] Petri net

[۱۲] Discrete Event Components with Priority