



پردیس علوم  
دانشکده ریاضی، آمار و علوم کامپیوتر

# بهبود روش واریسی مدل با استفاده از نظریه تعبیر مجرد

نگارنده

پویا پرتو

استاد راهنمای اول: دکتر مجید علی زاده  
استاد راهنمای دوم: دکتر مجتبی مجتهدی

پایان نامه برای دریافت درجه کارشناسی ارشد  
در رشته علوم کامپیوتر

تاریخ دفاع

## چکیده

روش وارسی مدل یک روش قابل اعتماد برای بررسی صحت عملکرد برنامه‌های کامپیوتری است. بیان‌های مختلف این روش از منطق موجهات بهره می‌برند که چندان برای برنامه نویسان شناخته شده نیستند. در این رساله سعی شده یک بیان جدید از روش وارسی مدل شرح داده شود که در آن به کمک نظریه تعبیر مجرد به جای منطق موجهات از عبارات منظم استفاده شده.

در این نوشته ابتدا به بیان مفاهیم اولیه برای بیان جدید روش وارسی مدل پرداخته‌ایم سپس این روش را به سه صورت متفاوت بیان کرده‌ایم. صورت اول ساختار خاصی ندارد و صرفاً روش در ادبیاتی نو بیان شده، صورت دوم ساختار عبارات منظم را به صورت‌بندی‌اش اضافه کرده و صورت سوم ساختار برنامه‌ها را به صورت‌بندی اضافه کرده تا روش به پیاده سازی نزدیک شود و معادل بودن این سه صورت نشان داده شده.

کلمات کلیدی: وارسی مدل، نظریه تعبیر مجرد، معناشناسی دلالتی، پیوند گالوا، درستی یابی صوری، تحلیل ایستا، درستی یابی برنامه‌های کامپیوتری

## تقديم به

## تقديم به

بورات صاگديف، نورسلطان تولياكبای و اورکين د ريپيست

سپاسگزاری

سپاسگزاری

## پیشگفتار

با توجه به پیشرفت روز افزون علوم کامپیوتر و ورود کاربردهای آن به زندگی روزمره، پیشرفت در روش‌های ساخت و نگه‌داری برنامه‌ها نیازی آشکار به نظر می‌رسد. یکی از مسائل مهم در این زمینه بررسی صحت کارکرد برنامه‌های نوشته‌شده است. عدم صحت کارکرد برنامه‌های نوشته‌شده بسته به حساسیت کاری که یک برنامه انجام می‌دهد می‌تواند تبعات مختلفی داشته‌باشد. پرتاب ناموفق آریان ۵ [۱۷]، از مدار خارج شدن مدارگرد مریخ [۲] و تصادف هلیکوپتر چینوک [۱] چند نمونه از تبعات بزرگ این قضیه در گذشته بوده‌اند، هرچند که به‌سادگی می‌توان فجایع دیگری را مشابه این اتفاقات در زندگی روزمره‌ی انسان‌ها متصور شد. برای کشف صحت کارکرد برنامه‌های کامپیوتری روش‌های متفاوتی ابداع شده‌اند که در ادامه به طور مختصر از آن‌ها یاد می‌کنیم اما پیش از آن به یک خاصیت مشترک همه‌ی این روش‌ها می‌پردازیم که ناکامل بودن است. منظور از ناکامل بودن این است که با استفاده از هیچ یک از روش‌هایی که داریم نمی‌توانیم هر خاصیتی را برای هر برنامه‌ای بررسی کنیم. به عبارت دیگر استفاده از هر روشی، محدودیت‌هایی دارد. و البته قضیه رایس [۲۱] به ما این تضمین را داده که روش کاملی اصلاً وجود ندارد. قضیه رایس به طور غیر رسمی بیان می‌کند که مسئله‌ی بررسی هر خاصیت غیر بدیهی، برای همه‌ی برنامه‌ها، تصمیم ناپذیر است. این دلیلی بر این شده که روش‌های مختلفی برای این کار درست شوند که هر کدام می‌توانند حالت‌های خاصی از مسأله را حل بکنند.

یک دسته‌بندی برای این روش‌ها تقسیم آن‌ها به دو دسته‌ی پویا و ایستا است. روش‌های پویا روش‌هایی هستند که در آن‌ها تست برنامه با اجرای برنامه همراه است و روش‌های ایستا بدون اجرای برنامه‌ها انجام می‌شوند. روش‌های پویا معمولاً با اجرای حالات محدودی از برنامه، تصمیم می‌گیرند که برنامه‌ای که نوشته‌ایم، انتظاراتمان را برآورده می‌کند یا خیر. اگر این روش بتواند تشخیص دهد برنامه‌ای درست کار نمی‌کند می‌توانیم با اطمینان نتیجه بگیریم که برنامه غلط نوشته‌شده، اما اگر برنامه‌ای از تست‌های ساخته‌شده با این روش‌ها با موفقیت عبور کند، نمی‌توان اطمینان حاصل کرد که برنامه درست کار می‌کند، زیرا ممکن است حالتی مشکل‌زا از اجرای برنامه وجود داشته باشد که در تست‌ها نیامده باشد. در کتاب [۱۹] به توضیح این روش‌ها پرداخته شده. این دسته از روش‌ها از موضوع اصلی کار ما دور هستند. روش‌های ایستا معمولاً روش‌هایی هستند که از

نظریه‌های مختلف در منطق ریاضی به عنوان ابزار بهره می‌برند تا بدون اجرای خود برنامه‌ها در مورد صحت اجرای آن‌ها نتیجه‌گیری کنند. به همین دلیل به بخشی مهم و بزرگی از این دستورات که از منطق استفاده می‌کنند روش‌های صوری هم گفته می‌شود. از معروف‌ترین این روش‌ها واریسی مدل، روش‌های استنتاجی و استفاده از نظریه تعبیر مجرد است. در روش واریسی مدل، یک مدل صوری متناهی از برنامه‌ی مورد بررسی می‌سازیم که همه‌ی حالات اجرای برنامه با آن قابل توصیف است، سپس با استفاده از یک زبان صوری که بتواند در مورد مدل‌هایمان صحبت کند، ویژگی‌های مورد بررسیمان را بیان می‌کنیم و در نهایت صحت ویژگی‌های بیان شده را بررسی می‌کنیم. مقاله [۴] شروع این روش‌ها بوده که این کار را با استفاده از نوعی مدل کریپکی [۱۶] و نوعی منطق زمانی به نام منطق زمانی خطی [۴] انجام داده که روشی است با دقت و البته هزینه‌ی محاسباتی بسیار بالا. [۱۲] یک منبع بسیار مقدماتی در این زمینه و کتاب [۵] یک مرجع سنتی در این زمینه است. در روش‌های استنتاجی که شاید بتوان یکی از ابتدایی‌ترین آن‌ها را استفاده از منطق هور [۱۱] دانست، درستی کارکرد برنامه‌هایمان را با ارائه‌ی یک درخت اثبات در یک دستگاه استنتاجی که متناسب با زبان برنامه‌هایمان ساخته شده، نشان می‌دهیم. در این روش هم اگر بتوانیم درستی یک برنامه را اثبات کنیم، دیگر به‌طور تئوری، خیالی آسوده از درستی برنامه خواهیم داشت اما ساختن درخت اثبات در یک نظریه برهان می‌تواند چالش برانگیز باشد چون این یک مسئله‌ی NP-Hard است. در [۱۲] به منطق هور به‌طور مقدماتی پرداخته شده. همین‌طور کتاب [۲۰] نیز به پیاده‌سازی منطق هور در زبان coq پرداخته. coq نیز یک اثبات‌یار است که بر اساس یک نظریه نوع وابسته کار می‌کند. برای اطلاعات بیشتر در مورد چگونگی طرز کار این اثبات‌یار و تئوری بنیادین آن می‌شود به کتاب [۳] مراجعه کرد. تئوری مورد شرح در [۱۰] نیز می‌تواند در این مسیر به کار گرفته شود. نظریه تعبیر مجرد [۸] نیز یک نظریه ریاضیاتی است که در این بحث می‌توان گفت، به‌نوعی سعی می‌کند از روی معناشناسی یک برنامه‌ی کامپیوتری [۲۳]، یک تقریب بسازد. منظور از تقریب، یک دستگاه کوچک‌تر از معناشناسی اصلی است که رفتارش زیرمجموعه‌ی رفتارهای دستگاه اصلی است. سعی بر این است که دستگاه جدیدی که می‌سازیم به لحاظ محاسباتی هم ساده‌تر از معناشناسی اصلی کار کند تا بتوانیم خواص آن را راحت‌تر بررسی کنیم. در این صورت هر نتیجه‌ای که در مورد خواص جدید بگیریم را می‌توانیم در مورد خود برنامه هم بیان کنیم اما می‌دانیم که در این صورت هم به همه‌ی حقایق دست پیدا نکرده ایم. در مورد این نظریه نیز به‌تازگی کتاب [۷] منتشر شده که حاصل نزدیک به ۵ دهه کار مبدع این نظریه، پاتریک کوزو، است. همین‌طور [۱۴] نیز در مورد پیاده‌سازی این نظریه بحث کرده.

# فهرست مطالب

۱	برخی مفاهیم اولیه	۱
۱	۱.۱ نظریه تعبیر مجرد	۱
۲	۲.۱ روش واریسی مدل	۲
۲	۱.۲.۱ زبان LTL	۲
۳	۲.۲.۱ معنانشناسی LTL	۳
۵	۲ صورتی‌گری جدید برای روش واریسی مدل	۵
۵	۱.۲ نحو زبان مورد بررسی	۵
۷	۲.۲ معنانشناسی زبان مورد بررسی	۷
۷	۱.۲.۲ برچسب‌ها	۷
۸	۲.۲.۲ رد پیشوندی	۸
۸	۳.۲.۲ تعریف صورتی معنانشناسی رد پیشوندی	۸
۱۲	۳.۲ ویژگی‌های معنایی برنامه‌ها	۱۲
۱۲	۱.۳.۲ ویژگی‌های معنایی	۱۲
۱۲	۲.۳.۲ عبارات منظم	۱۲
۱۳	۳.۳.۲ زبان عبارات منظم	۱۳
۱۵	۴.۳.۲ معنانشناسی عبارات منظم	۱۵
۱۷	۵.۳.۲ واریته‌های مختلف زبان عبارات منظم	۱۷
۱۸	۴.۲ صورت جدید مسئله‌ی واریسی مدل	۱۸
۲۰	۵.۲ در مورد توقف پذیری	۲۰
۲۴	۳ واریسی مدل منظم	۲۴
۲۴	۱.۳ در مورد عبارات منظم	۲۴
۲۴	۱.۱.۳ هم‌ارزی عبارات منظم	۲۴
۲۵	۲.۱.۳ فرم نرمال فصلی	۲۵
۲۹	۴ واریسی مدل ساختارمند	۲۹

۵ نتیجه گیری

۳۰



# فصل ۱

## برخی مفاهیم اولیه

در این فصل سعی شده خواننده با مفاهیم مقدماتی کار آشنا شود. بعضی از مفاهیم ممکن است مستقیماً در ادامه استفاده شده باشند و بعضی دیگر ممکن است مستقیماً در ادامه وارد بحث نشده باشند اما آشنایی با آنها برای درک بهتر واجب است.

### ۱.۱ نظریه تعبیر مجرد

نظریه ترتیب مجرد

تعریف ۱.۱. (ترتیب جزئی): اگر  $P$  یک مجموعه باشد و  $\leq$  یک رابطه روی این مجموعه باشد به‌طوری‌که:

$$1. \forall a \in P : a \leq a$$

$$2. \forall a, b \in P : (a \leq b \wedge b \leq a) \rightarrow a = b$$

$$3. \forall a, b, c \in P : a \leq b \wedge b \leq c \rightarrow a \leq c$$

آنگاه به زوج  $(P, \leq)$  یک ترتیب جزئی می‌گوییم.

در ادامه خواهیم دید که معنای برنامه‌های کامپیوتری که به یک زبان برنامه نویسی نوشته می‌شوند را می‌شود به شکل یک ترتیب جزئی دید. ترتیب‌های جزئی به عنوان یک نظریه ریاضی مطالعه شده‌اند و اگر معناسازی یک برنامه را بتوانیم به این شکل بیان کنیم می‌توانیم از خصوصیات که در مورد ترتیب جزئی می‌دانیم در جهت کار با معناسازی استفاده کنیم.

تعریف ۲.۱. (پیوند گالوا): اگر  $(C, \sqsubseteq)$  و  $(A, \preceq)$  دو ترتیب جزئی باشند و دو تابع  $\alpha : C \rightarrow A$  و  $\gamma : A \rightarrow C$  را داشته باشیم که:

$$\forall c \in C : \forall a \in A : \alpha(c) \preceq a \leftrightarrow c \sqsubseteq \gamma(a)$$

## ۲.۱ روش واری مدل

روش واری مدل یک روش صوری است که برای درستی یابی سیستم های مختلف استفاده می شود. در این روش معمولاً ابتدا یک ماشین حالات متناهی از روی سیستم مورد بررسی ساخته می شود، سپس بررسی هایی که قرار است روی سیستم اصلی انجام شوند، روی این ماشین (مدل) انجام می شود. در بررسی صحت کارکرد برنامه های کامپیوتری از این روش استفاده می شود اما این تنها مورد استفاده از این روش نیست و هر منظومه دیگری که قابلیت بیان به صورت صوری را داشته باشد قابل بررسی با این روش هست. مثلاً می توان از این روش برای بررسی صحت عملکرد برنامه ی قطارهای شهری استفاده کرد؛ در حالتی که مثلاً خصوصیات مورد بررسی ما عدم رخ دادن تصادف بین قطارها یا پوشش تمام مناطق شهر باشد. مثال های دیگر استفاده ی این روش در علوم کامپیوتر می تواند بررسی صحت عملکرد یک پردازنده یا مثلاً الگوریتم تقسیم وظایف یک سیستم عامل باشد. این مثال ها هیچ یک برنامه ی کامپیوتری نیستند (هر چند که ممکن است مجبور باشیم از یک برنامه ی کامپیوتری برای پیاده سازی آن ها کمک بگیریم که در آن صورت بررسی صحت عملکرد آن برنامه ی کامپیوتری داستانی دیگر خواهد داشت) اما قابل بیان به صورت صوری به جای زبان طبیعی هستند.

ایده ی روش واری مدل از منطق های زمانی مختلف استفاده می کند. منطق زمانی یک نوع منطق موجهات است. منطق های موجهات از گسترش زبان منطق کلاسیک با اضافه کردن ادوات وجهی گوناگون، با معانی متفاوتی که ممکن است در زبان طبیعی داشته باشند، ساخته می شوند. این ادوات غالباً در زبان طبیعی نقش قید را دارند. منطق های زمانی بخشی از منطق های موجهات هستند که به صوری گری ما مفهوم زمان را هم اضافه می کنند، یعنی قیدهایی مانند فعلاً، بعداً و قبلاً. منطقی که در اینجا بیان می کنیم LTL نام دارد که یکی از منطق های زمانی است که برای روش واری مدل استفاده می شود. البته در مورد قیدهایی که نام بردیم ذکر این نکته ضروری است که در این بیانی که ما در اینجا از این منطق ارائه داده ایم ادوات جدید این فعل ها نیستند، هر چند که به کمک ادوات جدید می توان ادواتی برای هر یک از این قیود ساخت. این تکه از [۱۸] آورده شده. ابتدا زبان این منطق را بیان می کنیم و سعی می کنیم به طور غیر دقیق در مورد معنای فرمول های این زبان به خواننده یک درک شهودی بدهیم؛ سپس به سراغ معناشناسی صوری این منطق می رویم.

### ۱.۲.۱ زبان LTL

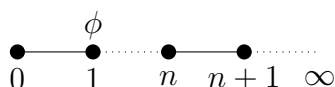
تعریف ۳.۱. هر عضو مجموعه ی  $\Phi$  یک فرمول در زبان LTL است (و  $\Pi$  مجموعه ی فرمول های اتمی است و  $\pi \in \Pi$ ):

$$\Pi \subset \Phi,$$

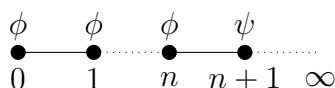
$$\phi \in \Phi \Leftrightarrow \phi ::= \pi | \phi \vee \phi | \neg \phi | \phi \bigcirc \phi | \phi \mathcal{U} \phi$$

اولین نکته‌ای که برای فرمول‌های این زبان به آن نیاز داریم این است که در این منطق ما زمان را با اعداد طبیعی و هر خاصیتی که در موردشان تعریف شده نشان می‌دهیم. یعنی برای یک فرمول، زمان از عدد ۰ شروع شده و تا ابد ادامه خواهد داشت و حین گذر زمان ممکن است ارزش فرمول‌ها تغییر کند. مسلماً پس از بررسی معناشناسی صوری بهتر می‌شود این مفهوم را به طور شهودی حس کرد، اما به هر حال به خواننده پیشنهاد می‌شود پیش از رسیدن به آن بخش به ادامه‌ی این بخش هم توجه شود.

در این زبان ادوات کلاسیک  $\neg, \vee$  هستند با همان معنایی که در منطق گزاره‌ای کلاسیک داشتند. در ادوات جدید  $\phi \circ \psi$  به معنای برقرار بودن این فرمول دقیقاً در لحظه‌ی بعدی (دقیقاً یک لحظه) است، مثلاً در شکل زیر با در نظر گرفتن اینکه در زمان ۰ هستیم، این فرمول در لحظه‌ی ۱ برقرار است.



$\phi \mathcal{U} \psi$  به این معنی است که فرمول سمت چپی حداقل تا قبل از اینکه فرمول سمت راستی برقرار شود، برقرار است. (مثلاً اگر بگوییم "تا وقتی که باران نباریده زمین خشک است" در این صورت "زمین خشک است" به جای فرمول سمت چپ و "باران باریده است" فرمول سمت راست است).



برای این زبان همان‌طور که در منطق کلاسیک از ادوات عطف و شرطی با اینکه با ادواتی که داریم قابل بیان هستند استفاده می‌کنند، ادوات بیشتری هم هستند که مورد استفاده قرار می‌گیرند و با همین دو ادواتی که معرفی کردیم قابل بیان هستند اما ما در اینجا از آن‌ها اسمی نیاورده‌ایم. دلیل وجود این‌ها هم راحت‌تر کردن کار کسی است که قرار است یک خاصیت را به صورت یک فرمول در این زبان بیان کند. همان‌طور که استفاده نکردن از یا و شرطی در منطق گزاره‌ای می‌تواند به سخت کردن بیان جملات در چارچوب این منطق منجر شود، حذف این ادوات وجهی هم بیان خواص را در این منطق مشکل می‌سازد. اما از آنجاییکه ما صرفاً این بخش را برای معرفی این ایده قرار داده‌ایم، دیگر به بیان ادوات وجهی دیگر نپرداخته‌ایم.

حال که به درکی شهودی از معنای فرمول‌های این زبان رسیده‌ایم، به بیان صوری این مفاهیم می‌پردازیم.

## ۲.۲.۱ معناشناسی LTL

مدل‌های این منطق را به صورت توابع  $M : \mathbb{N}_0 \rightarrow P(\Pi)$  تعریف می‌کنیم. یعنی هر مدل یک تابع است که هر عدد طبیعی را به یک مجموعه از فرمول‌های اتمی می‌برد. این در واقع قرار است به این

معنی باشد که یک مدل به تعبیری به این معنی است که در هر لحظه کدام یک از فرمول‌های اتمی درست هستند. مثلاً در مدلی به نام  $M_i$  در واقع  $M_i(5)$  مجموعه‌ی اتم‌هایی است که در لحظه‌ی ۵ طبق این مدل درست هستند و اگر اتمی در این مجموعه نباشد ارزش غلط دارد. درستی یک فرمول در یک مدل را با  $M, i \models \phi$  نشان می‌دهیم و  $M, i \models \phi$  به این معنی است که در لحظه‌ی  $i$  در مدل  $\phi$  ارزش درست دارد. این مفهوم را به صورت بازگشتی به شکل زیر تعریف می‌کنیم:

$$\begin{aligned}
M, i \models \pi & \text{ iff } \pi \in M(i) \\
M, i \models \neg\phi & \text{ iff } M, i \not\models \phi \\
M, i \models \phi \vee \psi & \text{ iff } M, i \models \phi \text{ or } M, i \models \psi \\
M, i \models \bigcirc\phi & \text{ iff } M, i+1 \models \phi \\
M, i \models \phi \mathcal{U} \psi & \text{ iff } \exists k \geq i \in \mathbb{N}_0 : \forall i \leq j < k : M, j \models \phi \text{ and } M, k \models \psi
\end{aligned}$$

برای یک فرمول اگر مدلی وجود داشته باشد که در آن مدل آن فرمول صادق باشد، آنگاه آن فرمول را ارضاپذیر می‌گوییم. اگر یک فرمول در هر مدلی صادق باشد، آن فرمول را معتبر می‌گوییم. شیوه‌ی دیگری برای بیان همین معناشناسی که گفتیم به شکل اتوماتا است.

## فصل ۲

# صوری‌گری جدید برای روش واریسی مدل

محوریت کار ما قرار است [۶] باشد که در آن سعی شده روش واریسی مدل با کمک نظریه تعبیر مجرد، بهبود داده شود. در [۴] روشی که معرفی شده در واقع ویژگی برنامه‌ها را به کمک منطق‌های LTL یا CTL بیان می‌کند. خود برنامه‌ها هم با کمک معنانشناسی این منطق‌ها که نوع خاصی از مدل‌های کرپسکی به اسم سیستم‌گذار هستند توصیف می‌شوند. اما در [۶] کاری که انجام شده به این شکل است که منطق‌های LTL و CTL با عبارات منظم [۱۵] جایگزین شده‌اند. علت این کار دو نکته بوده، اولی اینکه استفاده از عبارات منظم به جای منطق‌های نام برده شده می‌تواند برای برنامه نویسان ساده‌تر باشد و دومی اینکه عبارت منظم از منطق‌های نام برده شده قدرت بیان بالاتری دارد. [۲۴] در ادامه ی کار واریسی مدل با استفاده از موجودات جدید تعریف شده به سه شکل مختلف بیان شده. در هر مرتبه بیان واریسی مدل، به‌گفته‌ی نویسنده، ”ساختارمند” تر شده. می‌توان دریافت که فایده ساختارمندتر بودن بیان این است که پیاده‌سازی راحت‌تری دارد. حال به بیان و بررسی تعاریف و خواص آن‌ها می‌پردازیم.

### ۱.۲ نحو زبان مورد بررسی

زبان بیان برنامه‌ها زیرمجموعه‌ای از دستورات زبان C است، به شکل زیر:

$$x, y, \dots \in \mathbb{X}$$

$$A \in \mathbb{A} ::= 1 \mid x \mid A_1 - A_2$$

$$B \in \mathbb{B} ::= A_1 < A_2 \mid B_1 \text{ nand } B_2$$

$$E \in \mathbb{E} ::= A \mid B$$

$$S \in \mathbb{S} ::=$$

$$\begin{aligned}
 & x \doteq A; \\
 & | \ ; \\
 & | \text{ if } (B) \ S \mid \text{ if } (B) \ S \text{ else } S \\
 & | \text{ while } (B) \ S \mid \text{ break}; \\
 & | \{SI\} \\
 & SI \in \mathbb{SL} ::= SI \ S \mid \epsilon \\
 & P \in \mathbb{P} ::= SI
 \end{aligned}$$

در اینجا زیر مجموعه‌ای از دستورات زبان C را داریم. همین‌طور که قابل مشاهده است این زبان تا حد ممکن کوچک شده. علت این کار را بعداً عمیق‌تر حس خواهیم کرد. علت ساده‌تر شدن کار برای ارائه‌ی معنانشناسی و تعبیر مجرد آن است. در اینجا راحتی آن برنامه‌نویسی که قرار است با این زبان برنامه بنویسد مطرح نبوده چون اصلاً این زبان برای این کار ساخته نشده. نویسنده‌ی [۶] در اینجا صرفاً می‌خواسته فرآیند را نشان دهد. اگر به فرض برای زبانی مانند پایتون بخواهیم درستی‌یابی با استفاده از روش ارائه شده را درست کنیم، می‌توانیم همه‌ی راهی که در [۶] برای زبان توصیف شده، رفته‌شده را برای پایتون هم برویم و به یک تحلیل‌گر ایستا برای پایتون برسیم. در مورد قدرت بیان این زبان هم می‌توانیم بگوییم که می‌توانیم باقی اعداد را از روی عدد ۱ و عملگر منها بسازیم. مثلاً ابتدا ۰ را به کمک ۱-۱ می‌سازیم و سپس با استفاده از ۰ می‌توانیم یکی یکی اعداد منفی را بسازیم و سپس بعد از آن به سراغ اعداد مثبت می‌رویم که با کمک ۰ و هر عدد منفی‌ای که ساختیم، ساخته می‌شوند. باقی اعداد و حتی باقی عملگرها (یعنی به غیر از اعداد طبیعی) نیز از روی آنچه داریم قابل ساختن است. در مورد عبارت‌های بولی نیز داستان به همین منوال است. یعنی اینجا صرفاً ادات شفر تعریف شده و باقی عملگرهای بولی را می‌توان با استفاده از همین عملگر ساخت. باقی دستورات نیز دستورات شرط و حلقه هستند. باقی دستورات قرار است مطابق چیزی که از زبان C انتظار داریم کار بکنند. در مورد دستور break ذکر این نکته ضروری است که اجرای آن قرار است اجرای برنامه را از دستوری بعد از داخلی‌ترین حلقه‌ای که break داخلش قرار دارد ادامه دهد. در پایان می‌توان ثابت کرد که این زبان هم قدرت با مدل دیویس [۹] است. توجه داریم که هرچه در این بخش در مورد معنای دستورات این زبان گفتیم، به هیچ وجه صوری نبود و صرفاً درک شهودی‌ای که از معنای اجرای هریک از دستورات داشتیم را بیان کردیم. بیان صوری معنای برنامه‌ها را، که برخلاف درک شهودی‌مان قابل انتقال به کامپیوتر است، در ادامه بیان خواهیم کرد. طبیعتاً این بیان صوری از روی یک درک شهودی ساخته شده‌است.

## ۲.۲ معنانشناسی زبان مورد بررسی

معنانشناسی زبانی را که در بخش پیش آوردیم با کمک مفاهیمی به نام برچسب و رد پیشوندی و عملگر چسباندن روی دو رود پیشوندی مختلف تعریف خواهیم کرد و نام این معنانشناسی نیز معنانشناسی رد پیشوندی است.

### ۱.۲.۲ برچسب‌ها

باوجود اینکه خود زبان C در قسمتی از زبان خود چیزهایی به نام برچسب دارد اما همین‌طور که در بخش پیشین دیدیم، در زبانی که اینجا در حال بحث روی آن هستیم خبری از برچسب‌ها نیست. اما برای تعریف صوری معنای برنامه‌ها، به شکلی که مورد بحث است، به آن‌ها نیاز است. در این بخش ابتدا به توضیحی مختصر در مورد برچسب‌ها در معنانشناسی زبان مورد بحث می‌پردازیم. تعاریف صوری دقیق این موجودات در پیوست [۶] آورده شده‌اند. از آوردن مستقیم این تعاریف در اینجا خودداری کرده‌ایم. البته در مورد معنای صوری برچسب‌ها هم ذکر این نکته ضروری است که نویسنده‌ی [۶] حتی به صورت صوری هم برای هر بخش از برنامه این کار را به طور دقیق انجام نداده و انجام این کار به طور دقیق‌تر را احتمالاً به کسی که قرار است یک پیاده‌سازی کامل از این روش داشته باشد سپرده.

در زبانمان S‌ها بخشی از موجودات موجود در زبان هستند. برچسب‌ها را برای S‌ها تعریف می‌کنیم. برچسب‌ها با کمک توابع labs, in, brks-of, brk-to, esc, aft, at تعریف می‌شوند. درواقع هر S به ازای بعضی از این توابع یک برچسب دارد و این‌ها درواقع نشان‌دهنده‌ی آن برچسب هستند. بعضی دیگر این توابع برای هر S ممکن است یک مجموعه از برچسب‌ها را تعیین کند و یکی از آن‌ها هم با گرفتن S یک مقدار بولی را برمی‌گرداند.

at[S] : برچسب شروع S.

aft[S] : برچسب پایان S، اگر پایانی داشته باشد.

esc[S] : یک مقدار بولی را بازمی‌گرداند که بسته به اینکه در S دستور break وجود دارد یا خیر، مقدار درست یا غلط را برمی‌گرداند.

brk-to[S] : برچسبی است که اگر حین S دستور break اجرا شود، برنامه از آن نقطه ادامه پیدا می‌کند.

brks-of[S] : مجموعه‌ای از برچسب break‌های S را برمی‌گرداند.

in[S] : مجموعه‌ای از تمام برچسب‌های درون S را برمی‌گرداند.

labs[S] : مجموعه‌ای از تمام برچسب‌هایی که با اجرای S قابل دسترسی هستند را برمی‌گرداند.

## ۲.۲.۲ رد پیشوندی

پس از تعریف برجسبها به سراغ تعریف رد پیشوندی می‌رویم. پیش از آن باید وضعیت‌ها و محیط‌ها را تعریف کنیم.

تعریف ۱.۲. (محیط): به ازای مجموعه مقادیر  $\mathbb{V}$  و مجموعه متغیرهای  $\mathbb{X}$  تابع  $\rho : \mathbb{X} \rightarrow \mathbb{V}$  را یک محیط می‌گوییم. مجموعه‌ی همه‌ی محیط‌ها را با  $\mathbb{E}\mathbb{V}$  نمایش می‌دهیم.

تعریف ۲.۲. (وضعیت): به هر زوج مرتب به ترتیب متشکل از یک برجسب  $l$  و یک محیط  $\rho$  یک وضعیت  $\langle l, \rho \rangle$  می‌گوییم. مجموعه‌ی همه‌ی وضعیت‌ها را با  $\mathbb{S}$  نشان می‌دهیم.

تعریف ۳.۲. (رد پیشوندی): به یک دنباله از وضعیت‌ها (با امکان تهی بودن) یک رد پیشوندی می‌گوییم.

هر رد پیشوندی یک دنباله است که قرار است توصیفی از چگونگی اجرای برنامه باشد. وضعیت‌ها همان‌طور که از نامشان پیداست قرار است موقعیت لحظه‌ای برنامه را توصیف کنند.  $l$  قرار است برجسب برنامه‌ی در حال اجرا باشد و  $\rho$  مقدار متغیرها را در آن موقع از اجرای برنامه نشان می‌دهد. دنباله‌های ما می‌توانند متناهی یا نامتناهی باشند. مجموعه‌ی ردهای پیشوندی متناهی را با  $\mathbb{S}^+$  و مجموعه‌ی ردهای پیشوندی نامتناهی را با  $\mathbb{S}^\infty$  نمایش می‌دهیم. مجموعه‌ی همه‌ی ردهای پیشوندی را هم با  $\mathbb{S}^{+\infty}$  نمایش می‌دهیم. باتوجه به آنچه گفتیم، یک عملگر چسباندن  $\bowtie$  را روی ردهای پیشوندی تعریف می‌کنیم.

تعریف ۴.۲. (عملگر چسباندن): اگر داشته باشیم  $\sigma_1, \sigma_2 \in \mathbb{S}$ ,  $\pi_1, \pi_2 \in \mathbb{S}^{+\infty}$  داریم:

$$\begin{array}{ll} \pi_1 \bowtie \pi_2 = \pi_1 & \text{اگر } \pi_1 \in \mathbb{S}^+ \text{ داریم} \\ \pi_1 \bowtie \pi_2 & \text{اگر } \sigma_1 \neq \sigma_2 \\ \pi_1 \sigma_1 \bowtie \sigma_1 \pi_2 = \pi_1 \sigma_1 \pi_2 & \text{اگر } \pi_1 \in \mathbb{S}^\infty \text{ داریم} \end{array}$$

همین‌طور  $\epsilon$  هم یک رد پیشوندی است که حاوی هیچ وضعیتی نیست. به عبارت دیگر یک دنباله‌ی تهی است.

## ۳.۲.۲ تعریف صوری معناسازی رد پیشوندی

در این بخش قرار است دو تابع  $A$  و  $B$  را به ترتیب روی عبارات حسابی و بولی زبانمان یعنی  $A$ ها و  $B$ ها تعریف کنیم سپس با کمک آنها  $\mathcal{S}^*$  را روی مجموعه‌ای از اجتماع معنای  $S$ ها و  $SI$ ها تعریف می‌کنیم. پس در نهایت هدف ما تعریف  $\mathcal{S}^*$  است.



تعریف ۵.۲. (معنای عبارات حسابی - تابع  $\mathcal{A}$ ): تابع  $\mathcal{A} : \mathbb{A} \rightarrow \mathbb{EV} \rightarrow \mathbb{V}$  را به صورت بازگشتی روی ساختار  $A \in \mathbb{A}$  به شکل زیر تعریف می‌کنیم:

$$\mathcal{A}[1]\rho = 1$$

$$\mathcal{A}[x]\rho = \rho(x)$$

$$\mathcal{A}[A_1 - A_2]\rho = \mathcal{A}[A_1]\rho - \mathcal{A}[A_2]\rho$$

تعریف ۶.۲. (معنای عبارات بولی - تابع  $\mathcal{B}$ ): تابع  $\mathcal{B} : \mathbb{B} \rightarrow \mathbb{EV} \rightarrow \mathbb{BOOL}$  را به صورت بازگشتی روی ساختار  $B \in \mathbb{B}$  به شکل زیر تعریف می‌کنیم:

$$\begin{aligned} \mathcal{B}[A_1 < A_2]\rho &= True && \text{اگر } \mathcal{A}[A_1]\rho \text{ کوچکتر از } \mathcal{A}[A_2]\rho \text{ باشد} \\ \mathcal{B}[A_1 < A_2]\rho &= False && \text{اگر } \mathcal{A}[A_1]\rho \text{ بزرگتر از } \mathcal{A}[A_2]\rho \text{ باشد} \\ \mathcal{B}[B_1 \text{ nand } B_2]\rho &= \neg(\mathcal{B}[B_1]\rho \wedge \mathcal{B}[B_2]\rho) \end{aligned}$$

طبعاً  $\neg$  و  $\wedge$  در فرازبان هستند.

در ادامه به تعریف  $\mathcal{S}^*$  می‌پردازیم. این کار را با تعریف  $\mathcal{S}^*$  روی هر ساخت  $S$  و  $SI$  انجام می‌دهیم. پیش از ادامه‌ی بحث باید این نکته را درمورد علامت‌گذاری‌هایمان ذکر کنیم که منظور از  $S ::= l \text{ break};$  این است که تاکید کرده‌ایم که  $S$  با برچسب  $l$  شروع شده‌است وگرنه همین طور که گفتیم  $l$  جزو زبان نیست.

تعریف ۷.۲. (معنای برنامه‌ها - تابع  $\mathcal{S}^*$ ): اگر  $S ::= \text{break};$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}^*[S] = \{\langle at[S], \rho \rangle \mid \rho \in \mathbb{EV}\} \cup \{\langle at[S], \rho \rangle \langle brk - to[S], \rho \rangle \mid \rho \in \mathbb{EV}\}$$

اگر  $S ::= x \doteq A;$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}^*[S] = \{\langle at[S], \rho \rangle \mid \rho \in \mathbb{EV}\} \cup \{\langle at[S], \rho \rangle \langle aft[S], \rho[x \leftarrow \mathcal{A}[A]\rho] \rangle \mid \rho \in \mathbb{EV}\}$$

اگر  $S ::= \text{if}(B) S_t$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}^*[S] = \{\langle at[S], \rho \rangle \mid \rho \in \mathbb{EV}\} \cup \{\langle at[S], \rho \rangle \langle aft[S], \rho \rangle \mid \mathcal{B}[B]\rho = False\}$$

$\cup \{ \langle at[S], \rho \rangle \langle at[S_t], \rho \rangle \pi | \mathcal{B}[B] \rho = True \wedge \langle at[S_t], \rho \rangle \pi \in \mathcal{S}[S_t] \}$   
 اگر  $S ::= \text{if}(B) S_t \text{else} S_f$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\begin{aligned} \mathcal{S}[S] &= \{ \langle at[S], \rho \rangle | \rho \in \mathbb{V} \} \\ \cup \{ \langle at[S], \rho \rangle \langle at[S_f], \rho \rangle \pi | \mathcal{B}[B] \rho = False \wedge \langle at[S_f], \rho \rangle \pi \in \mathcal{S}[S_f] \} \\ \cup \{ \langle at[S], \rho \rangle \langle at[S_t], \rho \rangle \pi | \mathcal{B}[B] \rho = True \wedge \langle at[S_t], \rho \rangle \pi \in \mathcal{S}[S_t] \} \end{aligned}$$

اگر  $SI ::= \exists$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}[SI] = \{ \langle at[SI], \rho \rangle | \rho \in \mathbb{V} \}$$

اگر  $SI ::= SI' \ S$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}[SI] = \mathcal{S}[SI'] \cup (\mathcal{S}[SI'] \bowtie \mathcal{S}[S])$$

اگر  $S ::= \text{while}(B) S_b$  باشد، ماجرا نسبت به حالات قبل اندکی پیچیده‌تر می‌شود. تابعی به اسم  $\mathcal{F}$  را تعریف خواهیم کرد که در حقیقت دو ورودی دارد. ورودی اول آن یک دستور حلقه است و ورودی دوم آن یک مجموعه. به عبارتی دیگر می‌توانیم بگوییم به ازای هر حلقه یک تابع  $\mathcal{F}$  جداگانه تعریف می‌شود که مجموعه‌ای از ردهای پیشوندی را می‌گیرد و مجموعه‌ای دیگر از همین موجودات را باز می‌گرداند. کاری که این تابع قرار است انجام دهد این است که انگار یک دور دستورات داخل حلقه را اجرا می‌کند و دنباله‌هایی جدید را از دنباله‌های قبلی می‌سازد. معنای یک حلقه را کوچکترین نقطه ثابت این تابع در نظر می‌گیریم. در ادامه تعریف  $\mathcal{F}$  آمده. با دیدن تعریف می‌توان به دلیل این کار پی برد. آن نقطه‌ای که دیگر  $\mathcal{F}$  روی آن اثر نمی‌کند یا حالتی است که در آن دیگر شرط حلقه برقرار نیست و اصولاً قرار نیست دستورات داخل حلقه اجرا شوند که طبق تعریف  $\mathcal{F}$  می‌توانیم ببینیم که  $\mathcal{F}$  در این حالت چیزی به ردهای پیشوندی اضافه نمی‌کند. یا اینکه حلقه به دستور  $\text{break};$  خورده که در آن صورت وضعیتی به ته ردهای پیشوندی اضافه می‌شود که برچسبش خارج از مجموعه برچسب دستورات حلقه است و همین اضافه کردن هر چیزی را به ته ردهای پیشوندی موجود، توسط  $\mathcal{F}$  غیرممکن می‌کند. بنابراین نقطه ثابت مفهوم مناسبی است برای اینکه از آن در تعریف صوری معنای حلقه استفاده کنیم. علت اینکه کوچکترین نقطه ثابت

را به عنوان معنای حلقه در نظر می‌گیریم هم این است که مطمئن هستیم کوچکترین نقطه ثابت، هر رد پیشوندی ای را در خود داشته باشد به معنای اجرای برنامه مرتبط است. برای درک بهتر این نکته می‌توان به این نکته توجه کرد که با اضافه کردن وضعیت‌هایی کاملاً بی‌ربط به اجرای برنامه به ته ردهای پیشوندی، که صرفاً برچسب متفاوتی با آخرین وضعیت هر رد پیشوندی دارند، نقطه ثابت جدیدی ساخته ایم. پس اگر خودمان را محدود به انتخاب کوچکترین نقطه ثابت نکنیم، به توصیفات صوری خوبی از برنامه‌ها دست پیدا نخواهیم کرد. در مورد نقطه ثابت تنها این نکته باقی می‌ماند که اصلاً از کجا می‌دانیم که چنین نقطه ثابتی وجود دارد که در این صورت باید گفت مجموعه‌هایی که از ردهای پیشوندی تشکیل می‌شوند با عملگر زیرمجموعه بودن یک شبکه را تشکیل می‌دهند و بنا به قضیه تارسکی [۲۲] برای چنین موجودی نقطه ثابت وجود دارد. تعاریف موجوداتی که در موردشان صحبت کردیم به این شکل است:

$$\begin{aligned}\mathcal{S}[S] &= lfp^{\subseteq} \mathcal{F}[S] \\ \mathcal{F}[S]X &= \{\langle at[S], \rho \rangle | \rho \in \mathbb{EV}\} \cup \\ &\{\pi_2 \langle l, \rho \rangle \langle aft[S], \rho \rangle | \pi_2 \langle l, \rho \rangle \in X \wedge \mathcal{B}[B]\rho = False \wedge l = at[S]\} \cup \\ &\{\pi_2 \langle l, \rho \rangle \langle at[S_b], \rho \rangle \pi_3 | \pi_2 \langle l, \rho \rangle \in X \wedge \mathcal{B}[B]\rho = True \wedge \\ &\langle at[S_b], \rho \rangle \pi_3 \in \mathcal{S}[S_b] \wedge l = at[S]\}\end{aligned}$$

اگر  $S ::=$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}[S] = \{\langle at[S], \rho \rangle | \rho \in \mathbb{EV}\} \cup \{\langle at[S], \rho \rangle \langle aft[S], \rho \rangle | \rho \in \mathbb{EV}\}$$

اگر  $S ::= \{SI\}$  باشد، ردهای پیشوندی متناظر با اجرای این دستور را به شکل مجموعه‌ی زیر تعریف می‌کنیم:

$$\mathcal{S}[S] = \mathcal{S}[SI]$$

در ادامه چند مثال می‌زنیم تا مفهوم موجودات تعریف شده مشخص‌تر شود.

مثال ۸.۲.

مثال ۹.۲.

مثال ۱۰.۲.

## ۳.۲ ویژگی‌های معنایی برنامه‌ها

تا به اینجای کار یک زبان آورده‌ایم و برای آن معنا تعریف کرده‌ایم. در این فصل می‌خواهیم در مورد ویژگی‌های برنامه‌هایی که در این زبان نوشته می‌شوند با توجه به معنای صوری‌ای که تعریف کرده‌ایم، صحبت کنیم. دقت شود که برای برنامه‌هایی که در یک زبان برنامه‌نویسی نوشته می‌شوند می‌توان به اشکال مختلفی ویژگی تعریف کرد؛ مثلاً ویژگی‌های نحوی، مثل اینکه طول برنامه چند خط است یا هر کاراکتر چند بار به کار رفته، یا ویژگی‌های محاسباتی، مثل بررسی سرعت برنامه یا میزان استفاده‌ی آن از حافظه که عموماً در نظریه الگوریتم و پیچیدگی محاسبات بررسی می‌شود. منظور ما در اینجا از تعریف ویژگی، متناسب است با معناشناسی‌ای که برای برنامه‌هایمان تعریف کرده‌ایم. معناشناسی‌ای که تعریف کرده‌ایم در واقع سیر محاسباتی برنامه را توصیف می‌کند و ما می‌خواهیم ویژگی‌ها را با توجه به این موضوع تعریف کنیم. در این صورت می‌توانیم صحت عملکرد برنامه‌ها را با توجه به صادق بودن ویژگی‌هایی که در مورد آن‌ها تعریف شده بفهمیم. ابتدا به تعریف ویژگی‌ها می‌پردازیم، سپس به سراغ تعریف یک نوع عبارت منظم می‌رویم که از آن برای بیان ویژگی‌ها استفاده می‌شود.

## ۱.۳.۲ ویژگی‌های معنایی

همان‌طور که در بخش قبلی دیدیم، معنای هر برنامه با یک مجموعه‌ی  $S^*[S]$  مشخص می‌شود. وقتی می‌خواهیم ویژگی‌هایی را برای موجوداتی که به کمک مجموعه‌ها تعریف شده اند بیان کنیم، اینکه ویژگی‌ها را هم با مجموعه‌ها بیان کنیم کار معقولی به نظر می‌رسد. مثل اینکه بخواهیم ویژگی زوج بودن را در مورد اعداد طبیعی بیان کنیم. می‌توانیم مجموعه‌ی  $\mathbb{E}$  را به عنوان مجموعه‌ی همه‌ی اعداد زوج در نظر بگیریم و اینکه یک عدد زوج هست یا نه را عضویتش در مجموعه‌ی  $\mathbb{E}$  تعریف کنیم. پس یعنی در مورد اعداد طبیعی قرار است هر ویژگی به شکل زیرمجموعه‌ای از تمام این اعداد در نظر گرفته شود. یعنی هر عضو  $P(\mathbb{N})$  بنا به تعریف ما یک ویژگی از اعداد طبیعی است. در مورد برنامه‌ها نیز قرار است همین رویه را پیش بگیریم. تابع  $S^*$  از نوع  $P(\mathbb{S}^+) \rightarrow \mathbb{P}$  است. یعنی یک برنامه را در ورودی می‌گیرد و یک مجموعه از ردهای پیشوندی را باز می‌گرداند. پس می‌توانیم هر ویژگی را به عنوان زیر مجموعه‌ای از  $P(\mathbb{S}^+)$  تعریف کنیم، به عبارت دیگر عضوی از  $P(P(\mathbb{S}^+))$ .

## ۲.۳.۲ عبارات منظم

در اینجا توصیف ویژگی‌ها برای هر برنامه باید یک چارچوب داشته باشد. در صورت قدیمی روش واریسی مدل ما از منطق‌های زمانی برای بیان ویژگی‌ها به صورت صوری استفاده می‌کردیم و این احتیاج به یک زبان برای صوری کردن کامل کار را، که رسیدن به بیان مسئله‌ی واریسی مدل است،

به ما نشان می‌دهد. در اینجا ما با داستان دیگری هم رو به رو هستیم و آن این است که از آنجایی که با مجموعه‌ها سر و کار داریم و مجموعه‌ها چندان موجودات ساختنی‌ای نیستند (برخلاف مدل کریپکی)، بهتر است یک موجود ساختنی مثل یک زبان صوری برای بیان آن‌ها داشته باشیم. در این فصل قصد داریم یک نوع عبارت منظم را برای این منظور تعریف کنیم. پیشتر به نکته‌ی دیگری در مورد استفاده از عبارات منظم، که متداول‌تر بودن بین جامعه‌ی برنامه نویسان است، صحبت کردیم. ابتدا زبان این عبارت منظم را تعریف می‌کنیم، سپس به سراغ معناشناسی آن می‌رویم.

### ۳.۳.۲ زبان عبارات منظم

فرق عمده‌ای که زبان عبارات منظم ما با عبارات منظم کلاسیک دارد در کاراکترهاست. کاراکترها در زبان کلاسیک موجوداتی اتمی بودند، اما در اینجا ساختار دارند. در اینجا به جای هر کاراکتر یک زوج متشکل از مجموعه‌ی  $L$  و عبارت بولی  $B$  تشکیل شده‌اند که این زوج را به شکل  $L : B$  در زبانمان نمایش می‌دهیم. زبان ما به شکل BNF زیر است:

تعریف ۱۱.۲.

$$L \in P(\mathbb{L})$$

$$x, y, \dots \in \mathbb{X}$$

$$\underline{x}, \underline{y}, \dots \in \underline{\mathbb{X}}$$

$$B \in \mathbb{B}$$

$$R \in \mathbb{R}$$

$$\begin{aligned}
R ::= & \varepsilon \\
& | L : B \\
& | R_1 R_2 \quad (or \ R_1 \bullet R_2) \\
& | R_1 \mid R_2 \quad (or \ R_1 + R_2) \\
& | R_1^* \\
& | R_1^+ \\
& | (R_1)
\end{aligned}$$

همان طور که قابل مشاهده است در اینجا عملگرهای دوتایی چسباندن (•) و انتخاب (|) را داریم، به همراه عملگرهای یگانی \* و +. در ادامه خواهیم دید که در فرازبان معنی عملگر یگانی + به وسیله‌ی عملگر یگانی دیگر قابل بیان است، هرچند که در زبانمان هم برای سهولت کار از بیان این عملگر اجتناب نشده. توجه شود که پرائنترها هم جزئی از زبان قرار داده شده‌اند. همین‌طور در اینجا می‌خواهیم از تعدادی عبارات مخفف که در ادامه کارمان را راحت‌تر می‌کنند صحبت کنیم. منظور از زوج  $B : ?$  همان  $B : \mathbb{L}$  است. عبارت  $B : l$  به جای عبارت  $B : \{l\}$  به کار می‌رود و منظور از عبارت  $B : l$  نیز عبارت  $B : \mathbb{L} \setminus \{l\}$  است. با یک نگاه به دستور این زبان یک نکته‌ی چشمگیر برای ما، با توجه به موجوداتی که در بخش قبل تعریف کردیم، با نگاه به قواعد این زبان می‌تواند وجود یک مجموعه‌ی  $\mathbb{X}$  در کنار  $\mathbb{L}$  که از قبل داشتیم باشد. قرار است به ازای هر  $x \in \mathbb{X}$  یک  $x \in \mathbb{X}$  داشته باشیم. منظور از  $x$  مقدار متغیر  $x$  در ابتدای هر برنامه است. این یعنی تابع  $\rho : \mathbb{X} \rightarrow \mathbb{V}$  که  $\mathbb{V}$  مجموعه‌ی مقادیر متغیرهاست (در بخش قبل به این اشاره نشد اما خود  $\rho$  هایی که در بخش قبل داشتیم هم از نوع  $\mathbb{V} \rightarrow \mathbb{X}$  بود. با توجه به زبانمان و توضیحاتی که در گذشته دادیم، می‌توان در نظر گرفت که در اینجا  $\mathbb{V}$  همان اعداد صحیح است). همان‌طور که پیش‌تر گفتیم برای اشاره به یک تابع  $\rho$  از کلمه‌ی ”محیط“ استفاده می‌شود. به همین منوال در ادامه برای اشاره به  $\rho$  از ”محیط اولیه“ استفاده می‌کنیم. برای اشاره به مجموعه‌ی محیط‌های اولیه هم از نماد  $\mathbb{E}\mathbb{V}$  استفاده می‌کنیم. بقیه‌ی موجودات از جمله برچسب‌ها و عبارات بولی را هم که قبلاً داشتیم. در ادامه به بیان صوری معنای زبان بیان شده می‌پردازیم. پس از آن می‌توانیم با بررسی چند مثال، از اینکه معنای هر عبارت منظم چیست درکی شهودی به دست آوریم.

## ۴.۳.۲ معناسازی عبارات منظم

معنای عبارات منظم را با استفاده از تابع  $S^r$  نشان می‌دهیم. این تابع به این شکل تعریف می‌شود که در ورودی یک عبارت منظم  $R$  را می‌گیرد، سپس یک مجموعه از زوج مرتب‌های (یا همان‌طور که پیش‌تر نام‌گذاری کردیم "وضعیت‌ها"ی)  $\langle \rho, \pi \rangle$  را که  $\rho \in \mathbb{EV}$  و  $\pi \in S^*$  باز می‌گرداند. بنابراین این تابع از نوع  $\mathbb{R} \rightarrow P(\mathbb{EV} \times S^*)$  است. همین‌طور دقت شود که تا به حال از  $S^*$  صحبتی نکرده بودیم و فقط  $S^+$  را معرفی کرده بودیم.  $S^*$  نیز برابر است با  $S^+ \cup \{\epsilon\}$  (به لحاظ معنایی همان عملگر  $*$  است که در زبان عبارات منظم هست، مشهور به ستاره‌ی کلینی).  
تعریف استقرایی تابع  $S^r$  به شکل زیر است:

تعریف ۱۲.۲. تابع  $S^r : \mathbb{R} \rightarrow P(\mathbb{EV} \times S^*)$  به صورت استقرایی روی ساختار عبارت منظم  $R$  به صورت زیر تعریف می‌شود:

$$S^r[\epsilon] = \{\langle \rho, \epsilon \rangle \mid \rho \in \mathbb{EV}\}$$

[یعنی معنای عبارت منظم  $\epsilon$  مجموعه‌ای شامل زوج مرتب‌هایی از محیط‌های اولیه‌ی مختلف در کنار رد پیشوندی تهی استفاده می‌کند.]

$$S^r[L : B] = \{\langle \rho, \langle l, \rho \rangle \rangle \mid l \in L \wedge B[B]\rho, \rho\}$$

[این یعنی معنای عبارت  $S^r[L : B]$  زوج مرتب‌هایی هستند که عضو اول آن‌ها محیط‌های اولیه مختلف هستند) مانند مورد قبلی و البته در موارد آتی! و عضو دوم آن‌ها ردهای پیشوندی تک‌عضوی  $\langle l, \rho \rangle$  هستند که در آن‌ها برچسب  $l$  باید در  $L$  که مجموعه‌ای از برچسب‌هاست حضور داشته باشد و عبارت بولی  $B$  باید درباره‌ی محیط اولیه  $\rho$  و محیط  $\rho$  برقرار باشد. حتما متوجه این نکته شدید که  $B$  در اینجا به جای اینکه از نوع  $\mathbb{EV} \rightarrow \text{BOOL}$  باشد، همان‌طور که قبلا تعریف کردیم، از نوع  $\mathbb{EV} \rightarrow \mathbb{EV} \rightarrow \text{BOOL}$  است. (منظور از  $\text{BOOL}$  همان مجموعه‌ی  $\{True, False\}$  است.) در اینجا  $A$  و  $B$  را در ادامه با نوع‌های متفاوت دوباره تعریف خواهیم کرد، که البته فرق اساسی‌ای با تعریف قبلی ندارد و صرفا گسترشی ساده از آن است.]

$$S^r[R_1 R_2] = S^r[R_1] \bowtie S^r[R_2]$$

به‌طوری که در آن برای هر دو مجموعه‌ی  $S$  و  $S'$  از ردهای پیشوندی:

$$S \bowtie S' = \{\langle \rho, \pi \pi' \rangle \mid \langle \rho, \pi \rangle \in S \wedge \langle \rho, \pi' \rangle \in S'\}$$

[این یعنی اگر یک عبارت منظم داشته باشیم که از چسباندن  $R_1$  و  $R_2$  به هم ساخته شده باشد، آنگاه معنای این عبارت منظم با چسباندن ردهای پیشوندی موجود در مولفه‌ی دوم زوج مرتب‌هایی

که اعضای مجموعه‌ی معنای این دو عبارت منظم هستند و گذاشتن این رد پیشوندی‌های حاصل از چسباندن در معنای عبارت منظم جدید تعریف می‌شود. همین‌طور که می‌بینید یک عملگر چسباندن برای دو مجموعه از این زوج‌های  $\langle \rho, \pi \rangle$  تعریف شده و در تعریف  $S^r[R_1 R_2]$  از آن کمک گرفته شده.

تا این تکه از تعریف معنای عبارت منظم که رسیده‌ایم، تا حدی به دستیابی به درکی شهودی از اینکه به چه نحوی قرار است عبارات منظم راهی برای توصیف ویژگی در مورد برنامه‌ها باشد نزدیک‌تر شده‌ایم. همان‌طور که در مورد قبل دیدیم هر زوج  $L : B$  دقیقاً به یک وضعیت داخل یک رد پیشوندی اشاره می‌کند. انگار که قرار است این زوج‌ها موازی با وضعیت‌ها در ردهای پیشوندی موجود در معنای یک برنامه جلو روند و منطبق باشند تا واریسی مدل انجام شود. درک این موضوع اولین قدم ماست در دیدن عصاره‌ی روش واریسی مدل در ادبیاتی که از اول این فصل عَلم کرده‌ایم.

$$S^r[R_1 \mid R_2] = S^r[R_1] \cup S^r[R_2]$$

[این مورد معنای اعمال عملگر انتخاب روی دو عبارت منظم را توصیف می‌کند. معنای اعمال این عملگر به‌سادگی به صورت اجتماع معنای هر دو عبارت منظم تعریف شده.]

$$S^r[R]^0 = S^r[\varepsilon]$$

$$S^r[R]^{n+1} = S^r[R]^n \bowtie S^r[R]$$

[دو عبارت اخیر برای توصیف معنای عملگرهای  $*$  و  $+$  تعریف شده‌اند. عملگر  $\bowtie$  و معنای  $S^r[\varepsilon]$  را هم که قبلاً تعریف کرده بودیم و  $0$  و  $n$  و  $n+1$  هم اعداد طبیعی‌اند و  $+$  لاجرم همان جمع اعداد طبیعی است.]

$$S^r[R^*] = \bigcup_{n \in \mathbb{N}} S^r[R^n]$$

$$S^r[R^+] = \bigcup_{n \in \mathbb{N} \setminus \{0\}} S^r[R^n]$$

[این دو عبارت هم تعریف معنای خود دو عملگر  $*$  و  $+$  هستند. منظور از  $\mathbb{N}$  مجموعه‌ی اعداد طبیعی است. همان‌طور که قبل‌تر هم اشاره شد  $+$  را می‌توان در فرازبان با  $*$  تعریف کرد. اضافه می‌کنیم که خود  $*$  را هم در فرازبان می‌توان با عملگر انتخاب تعریف کرد و در اینجا می‌توان این نکته را هم دید.]

$$S^r[(B)] = S^r[B]$$

[این تکه از تعریف هم صرفاً بیان می‌کند که پرانتزها تاثیری در معنای عبارات منظم ندارند که کاملاً قابل انتظار است چرا که وجود پرانتز قرار است در صرفاً در خواص نحوی زبان اثر بگذارد.]



تعریف معنای عبارات منظم در اینجا تمام می‌شود اما همان‌گونه که در لابه‌لای تعاریف گفتیم، احتیاج داریم که  $A$  و  $B$  را از نو تعریف کنیم:

تعریف ۱۳.۲. توابع  $A : A \rightarrow \underline{EV} \rightarrow EV \rightarrow \mathbb{V}$  و  $B : B \rightarrow \underline{EV} \rightarrow EV \rightarrow \text{BOOL}$  به شکل استقرایی به ترتیب روی ساختارهای  $A \in A$  و  $B \in B$  به شکل زیر تعریف می‌شوند:

$$\begin{aligned} A[1]_{\underline{\rho}}, \rho &= 1 \\ A[x]_{\underline{\rho}}, \rho &= \underline{\rho}(x) \\ A[x]_{\underline{\rho}}, \rho &= \rho(x) \\ A[A_1 - A_2]_{\underline{\rho}}, \rho &= A[A_1]_{\underline{\rho}}, \rho - A[A_2]_{\underline{\rho}}, \rho \\ B[A_1 < A_2]_{\underline{\rho}}, \rho &= A[A_1]_{\underline{\rho}}, \rho < A[A_2]_{\underline{\rho}}, \rho \\ B[B_1 \text{ nand } B_2]_{\underline{\rho}}, \rho &= B[B_1]_{\underline{\rho}}, \rho \uparrow B[B_2]_{\underline{\rho}}, \rho \end{aligned}$$

به راحتی قابل مشاهده است که تعاریف جدید تا حد خوبی به تعاریف قبلی شبیه هستند و فرق عمده صرفاً وارد شدن  $\rho$  است. حال به سراغ چند مثال از عبارات منظم و معنای آن‌ها می‌رویم.

مثال ۱۴.۲. فرض کنید عبارت منظم ما

مثال ۱۵.۲. این سه تا مثال باید با سه تا مثال بخش معناشناسی برنامه‌ها سینک باشند! همین طور در ادامه بعد از تعریف مدل چکینگ در این فصل هم ۳ تا مثال خواهیم داشت که قراره هر کدومشون از این ۳ تا مثال و ۳ تا مثالی که قبلاً تعریف کردیم تشکیل شده باشند.

مثال ۱۶.۲.

تا اینجا کار بیشتر مفاهیمی که برای بیان صورت جدید مسئله‌ی واری واری مدل احتیاج داریم را بیان کرده‌ایم.

## ۵.۳.۲ واریته‌های مختلف زبان عبارات منظم

به عنوان قسمت آخر این بخش واریته‌های مختلفی از زبان عبارات منظم را بیان می‌کنیم. ، که هر کدام در واقع زیرمجموعه‌هایی از کل عبارات زبانی که توصیف کرده‌ایم را توصیف می‌کنند. بعضی از آن‌ها را در همین فصل برای هدف نهایی این فصل و بعضی دیگر را در فصل بعدی استفاده می‌کنیم.

اولین واریته‌ای که می‌خواهیم بیان کنیم، واریته‌ای است که در اعضای آن اصلاً عبارت  $L : B$  حضور ندارد و کل عبارت‌های زبان از  $\varepsilon$  ها تشکیل شده‌اند.

تعریف ۱۷.۲. (عبارت منظم تهی -  $\mathbb{R}_\varepsilon$ ):

$$R \in \mathbb{R}_\varepsilon$$

$$R ::= \varepsilon \mid R_1 R_2 \mid R_1 + R_2 \mid R_1^* \mid R_1^+ \mid (R_1)$$

با توجه به بخش قبل متوجه هستیم که معنای همه‌ی این عبارت‌ها برابر  $\{\langle \rho, \varepsilon \rangle\}$  خواهد بود. واریته‌ی بعدی عبارت منظم ناتهی است.

تعریف ۱۸.۲. (عبارت منظم ناتهی -  $\mathbb{R}^+$ ):

$$R \in \mathbb{R}^+$$

$$R ::= L : B \mid \varepsilon R_2 \mid R_1 \varepsilon \mid R_1 R_2 \mid R_1 + R_2 \mid R_1^+ \mid (R_1)$$

دلیل وجود  $\varepsilon R_2$  و  $R_1 \varepsilon$  در تعریف این است که ممکن است معنای عبارتی با معنای عبارات عضو  $\mathbb{R}_\varepsilon$  برابر نباشد (یعنی برابر  $\langle \rho, \varepsilon \rangle$  نباشد)، اما در خود عبارت  $\varepsilon$  حضور داشته باشد. با این تفصیل می‌توان دید که دو مجموعه‌ی  $\mathbb{R}_\varepsilon$  و  $\mathbb{R}^+$  یک افزاز برای مجموعه‌ی  $\mathbb{R}$  هستند، براساس اینکه معنای هر عبارت در  $\mathbb{R}$  برابر  $\langle \rho, \varepsilon \rangle$  هست یا خیر. بنابراین شاید به نظر برسد که تعریف یکی از آن‌ها به طور ساختاری کافی بود، اما ممکن است درجایی احتیاج داشته باشیم که ساختاری استقرایی روی هر یک از آن‌ها عَلم کنیم یا اینکه در اثبات حکمی بخواهیم از استقرا روی یکی از این دو ساختار استفاده کنیم.

واریته‌ی آخر عبارات منظم ما نیز عبارات منظم بدون انتخاب است.

تعریف ۱۹.۲. (عبارت منظم بدون انتخاب -  $\mathbb{R}^\dagger$ ):

$$R \in \mathbb{R}^\dagger$$

$$R ::= \varepsilon \mid L : B \mid R_1 R_2 \mid R_1^* \mid R_1^+ \mid (R_1)$$

## ۴.۲ صورت جدید مسئله‌ی واری مدل

بالاخره به هدف نهایی این فصل رسیدیم. می‌خواهیم صورت جدیدی از مسئله‌ی واری مدل را بیان کنیم.

پیش از ارائه‌ی تعریف واری مدل نیاز داریم تا عملگر بستار پیشوندی را برای یک مجموعه از ردهای پیشوندی معرفی کنیم.

تعریف ۲۰.۲. (بستار پیشوندی): اگر  $\Pi \in P(\mathbb{EV} \times \mathbb{S}^+)$  آنگاه بستار پیشوندی  $\Pi$  را به صورت زیر تعریف می‌کنیم:

$$\text{prefix}(\Pi) = \{ \langle \underline{\rho}, \pi \rangle \mid \pi \in \mathbb{S}^+ \wedge \exists \pi' \in \mathbb{S}^* : \langle \underline{\rho}, \pi \pi' \rangle \in \Pi \}$$

برای درک بهتر مفهوم بستار پیشوندی به مثال زیر توجه شود.

مثال ۲۱.۲. اگر  $\Pi = \{ \langle \underline{\rho}, \langle l_1, \rho_1 \rangle \langle l_2 \rho_2 \rangle \rangle \langle l_3, \rho_3 \rangle \rangle, \langle \underline{\rho}, \langle l_1', \rho_1' \rangle \langle l_2' \rho_2' \rangle \rangle \}$  باشد  $\Pi$  شامل دو عضو است) آنگاه:

$$\begin{aligned} \text{prefix}(\Pi) = \{ & \langle \underline{\rho}, \langle l_1, \rho_1 \rangle \rangle, \langle \underline{\rho}, \langle l_1, \rho_1 \rangle \langle l_2 \rho_2 \rangle \rangle, \langle \underline{\rho}, \langle l_1, \rho_1 \rangle \langle l_2 \rho_2 \rangle \langle l_3, \rho_3 \rangle \rangle, \\ & \langle \underline{\rho}, \langle l_1', \rho_1' \rangle \rangle, \langle \underline{\rho}, \langle l_1', \rho_1' \rangle \langle l_2' \rho_2' \rangle \rangle \} \end{aligned}$$

که شامل ۵ عضو است.

حال به ارائه‌ی صورت جدیدمان از روش واریسی مدل می‌رسیم که هدف اصلی این اصل بود و با این تعریف فصل تمام می‌شود.

تعریف ۲۲.۲. (واریسی مدل): اگر  $\underline{\rho} \in \mathbb{EV}, R \in \mathbb{R}^+, P \in \mathbb{P}$  آنگاه:

$$P, \underline{\rho} \models R \Leftrightarrow (\{\underline{\rho}\} \times \mathcal{S}^*[P]) \subseteq \text{prefix}(\mathcal{S}^*[R \bullet (? : T)^*])$$

این تعریف بیان می‌کند که برنامه‌ی  $P$  در صورتی که با محیط اولیه‌ی  $\underline{\rho}$  اجرا شود، در صورتی خاصیتی که با عبارت منظم  $R$  بیان شده را دارد که معنای آن زیرمجموعه‌ی بستار پیشوندی معنای عبارت منظم  $R \bullet (? : T)^*$  باشد. توجه شود که محیط اولیه‌ای که برای برنامه‌ی مورد بررسی متصور هستیم صرفاً به این منظور قرار داده شده که معنانشناسی برنامه را بتوانیم با معنای عبارات منظم قابل قیاس کنیم. دلیل حضور محیط اولیه در معنای عبارات منظم نیز در صورت سوم روش واریسی مدل یعنی فصل ۴ مشخص می‌شود و در این صورت از روش واریسی مدل و صورت بعدی آن چندان نقشی ندارد.

در مورد نقش  $(? : T)^*$  و  $\text{prefix}$  این به تصمیم مبدع این روش بوده که این دو در تعریف روش واریسی مدل حضور داشته باشند. حضور این دو طبعاً باعث می‌شود به ازای یک عبارت منظم  $R$  نسبت به این حالت که صرفاً معنی برنامه زیرمجموعه‌ی معنی  $R$  باشد، برنامه‌های بیشتری باشند که خاصیت بیان شده با  $R$  را ارضا کنند، چون در این صورت مجموعه‌ی سمت راستی در رابطه‌ی زیرمجموعه بودن بزرگتر می‌شود.

## ۵.۲ در مورد توقف پذیری

در این بخش مشکلی از کار که به نظر نگارنده رسیده مطرح شده. متأسفانه این مشکل بسیار بزرگ است و به نظر عجیب می‌آید که نویسنده‌ی [۶] متوجه آن نبوده! اگر صحبت ما در اینجا درست باشد، این به این معنی خواهد بود که کل کاری که در حال توصیفش هستیم قابل پیاده سازی نیست!

بحث ما در اینجا در مورد توقف پذیری است. در [۶] در مورد توقف یک برنامه صحبتی به میان نیامده. یعنی حتی گفته نشده که در چه صورتی می‌توانیم بگوییم که یک برنامه متوقف شده است. یک تعریف صوری معقول که خودمان می‌توانیم برای این معنا بیاوریم این است:

تعریف ۲۳.۲. برنامه‌ی  $P$  را به همراه اجرای اولیه  $\rho$  توقف پذیر می‌گوییم اگر و تنها اگر وجود داشته باشد  $\pi \in S^*[P]$  که

$$\pi = \langle at[P], \rho \rangle \pi'$$

و اینکه  $\langle aft[P], \rho \rangle$  در  $\pi$  حضور داشته باشد. این اتفاق را با  $P, \rho \downarrow$  نشان می‌دهیم.

در این تعریف توقف پذیری به متناهی بودن ردهای پیشوندی موجود در برنامه ربط داده نشده. با توجه به معنانشناسی‌ای که داریم، تعریف توقف پذیری به معنای وجود رد پیشوندی متناهی در معنای برنامه که اصلاً جور در نمی‌آید، چون معنانشناسی ما خاصیت پیشوندی بودن را دارد و مطمئن هستیم در معنای هر برنامه‌ای حتماً یک رد پیشوندی متناهی وجود دارد.

اگر هم بخواهیم تعریف توقف پذیری را وجودنداشتن ردهای پیشوندی نامتناهی در معنای برنامه در ابتدا به نظر می‌آید که به تعریف قوی‌تری نسبت به آنچه ارائه دادیم رسیده‌ایم. ما در اینجا سعی داریم تعریفی را ارائه کنیم که برای حرف‌هایی که در [؟] زده شده تا حد امکان مشکل درست نکند، که اگر دیدیم با این وجود مشکل وجود دارد مطمئن باشیم که اشتباه در [؟] است و نه حرف ما. پس سعی از ارائه‌ی این تعریف که به نظر از تعریف ارائه شده با کار ناسازگارتر می‌آید اجتناب می‌کنیم (در ادامه به بیان ناسازگاری پراخته شده) اما می‌بینیم که تعریفی که ارائه کردیم با همان که بگوییم در برنامه رد پیشوندی نامتناهی وجود ندارد معادل است.

قضیه ۲۴.۲. برای برنامه‌ی  $P$  و محیط اولیه‌ی  $\rho$  داریم  $P, \rho \downarrow$  اگر و تنها اگر

$$\forall \pi \in S^*[P] : \pi \in \mathbb{R}^+$$

اثبات. ( $\Rightarrow$ ) برای این قسمت باید ثابت کنیم که در معنای هر برنامه‌ای رد پیشوندی‌ای وجود دارد که به  $\langle aft[P], \rho \rangle$  ختم شده. در این اثبات از تعریف برجسب‌ها که در [۶] آمده استفاده شده. داریم  $P = SI$  و  $aft[P] = aft[SI]$  حکم را با استقرا روی ساختار  $SI$  ثابت می‌کنیم.

$$\blacktriangleleft SI = \epsilon :$$

داریم:

$$\mathcal{S}^*[\epsilon] = \{\langle at[\epsilon], \rho | \rho \in \mathbb{EV} \rangle\}$$

و طبق تعریف برجسبها داریم:

$$at[\epsilon] = aft[\epsilon]$$

پس حکم برقرار است.

$$\blacktriangleleft SI = SI' S :$$

اینکه در معنای SI دنباله‌ای شامل  $\langle aft[SI], \rho \rangle$  وجود داشته باشد، به با توجه به تعاریفی که داریم به این وابسته است که در معنای S دنباله‌ای شامل  $\langle aft[S], \rho \rangle$  وجود داشته باشد. برای اینکه این را ثابت کنیم هم باید همین حکم را روی ساختار S ثابت کنیم که در واقع بخش اصلی اثبات این سمت قضیه است.

$$\blacktriangleleft\blacktriangleleft S = x \doteq A; :$$

در این حالت با توجه به تعریف معنای S که قبل تر ارائه شد، دنباله‌ی

$$\langle at[S], \rho \rangle \langle aft[S], \rho[x \leftarrow \mathcal{A}[A]] \rho \rangle$$

در معنای دستور به ازای هر  $\rho$  وجود دارد که خب در هر صورت این شامل  $\rho$  هم می‌شود.

$$\blacktriangleleft\blacktriangleleft S = ; :$$

با توجه به معنای این دستوردنباله‌ی زیر در معنای این دستور وجود دارد.

$$\langle at[S], \underline{\rho} \rangle \langle aft[S], \underline{\rho} \rangle$$

$$\blacktriangleleft\blacktriangleleft S = \text{if}(B)S_t :$$

در صورتی که  $\mathcal{B}[B]\rho = T$  دنباله‌ی

$$\langle at[S], \underline{\rho} \rangle \langle at[S_t], \underline{\rho} \rangle \pi$$

در مجموعه‌ی معنای این دستور حضور دارد در حالیکه  $\langle at[S_t], \underline{\rho} \rangle \pi$  داخل معنای  $S_t$  است و طبق فرض استقرا می‌دانیم که برجسب آخرین موقعیت  $\pi$  برابر است با  $aft[S_t]$  که طبق تعاریف مربوط به برجسبها  $aft[S_t] = aft[S]$ . در صورتی که معنای عبارت بولی غلط باشد هم دنباله‌ی زیر در معنای دستور طبق تعریف موجود است.

$$\langle at[S], \underline{\rho} \rangle \langle aft[S], \underline{\rho} \rangle$$

$$\blacktriangleleft S = \text{if } (B) S_t \text{ else } S_f :$$

مانند حالت قبل است منتها با این تفاوت که در صورتی که معنای عبارت بولی غلط باشد دنباله‌ی زیر در معنای دستور حضور دارد:

$$\langle at[S], \rho \rangle \langle at[S_f], \rho \rangle \pi$$

و تساوی  $aft[S_t] = aft[S] = aft[S_f]$  هم طبق تعریف برچسب‌ها برقرار است.

$$\blacktriangleleft S = \text{while } (B) S_t :$$

در اثبات این سمت قضیه این حالت پیچیده ترین حالت است و در واقع تنها حالتی است که در اثبات آن به فرض قضیه احتیاج داریم! همان طور که پیشتر گفتیم معنای حلقه با استفاده از یک تابع تعریف می‌شود. معنای حلقه کوچکترین نقطه ثابت این تابع است، در حالیکه انگار این تابع وقتی روی یک مجموعه از ردهای پیشوندی اعمال شود، تاثیرات یک بار اجرای دستورات درون حلقه را روی ردهای پیشوندی درون مجموعه اعمال می‌کند.

طبق تعریف  $\mathcal{F}$  مطمئن هستیم که رد پیشوندی‌ای که با محیط  $\rho$  شروع شود در مجموعه‌ی معنای  $S$  وجود دارد، چونکه به ازای هر محیط  $\rho$  حالت  $\langle at[S], \rho \rangle$  در هر اعمال تابع  $\mathcal{F}$  روی هر مجموعه‌ی دلخواه وجود دارد. وقتی معنای  $S$  را به عنوان کوچکترین نقطه ثابت  $\mathcal{F}$  در نظر گرفته‌ایم پس مطمئن هستیم که آن مجموعه‌ای که کوچکترین نقطه ثابت است شامل رد پیشوندی  $\langle at[S], \rho \rangle$  است. این رد پیشوندی با اجرای  $\mathcal{F}$  تحت تاثیر قرار می‌گیرد. اگر معنای  $B$  در یکی از اعمال های  $\mathcal{F}$  غلط باشد، رد پیشوندی  $\langle aft[S], \rho \rangle \pi \langle at[S], \rho \rangle$  در معنای برنامه قرار خواهد گرفت و می‌توانیم بگوییم اجرای دستور با این محیط اولیه توقف پذیر است (توقف پذیری برای دستور را هم به همان معنی‌ای که برای برنامه‌ها گفتیم داریم به این شکل که کافی است دستور با برنامه در تعریف جایگزین شود). می‌دانیم که طبق تعریف تابع به انتهای این رد پیشوندی چیزی اضافه نمی‌شود. از طرف دیگر هم با این محیط اولیه، با توجه به تعریف رد پیشوندی دیگری وجود ندارد که طولانی‌تر از رد پیشوندی مورد اشاره باشد.

در حالت دیگر اگر فرض کنیم هیچ گاه به حالتی نمی‌رسیم که در آن معنای  $B$  غلط باشد هم با فرض مسئله به تناقض می‌خوریم، چون در آن صورت تابع  $\mathcal{F}$  مدام به طول دنباله‌هایی که با محیط اولیه‌ی  $\rho$  شروع می‌شوند می‌افزاید و این یک دنباله‌ی نامتناهی را خواهد ساخت. در صورتی که معنای  $B$  هیچ گاه صحیح نباشد، حداقل حالت  $\langle at[S_t], \rho \rangle$  به ته دنباله‌های پیشین اضافه خواهد شد و از این جهت مطمئن هستیم که دنباله‌ی نامتناهی گفته شده در معنای دستور حضور خواهد داشت.

پس با این تفصیل، این مورد هم ثابت می‌شود.

◀◀  $S = \text{break};$  :

در تعریف تابع  $aft$  روی برچسب‌ها این تعریف برای این دستور مشخص نیست! مهم‌ترین چیزی که در مورد برچسب‌ها در مورد این دستور قرار است برقرار باشد این است که اگر این دستور بخشی از  $S_t$  در حلقه‌ی زیر باشد

$$S = \text{while } B \ S_t$$

در این صورت  $aft[S] = brk - to[S_t]$  را طبق تعریف داریم. انتظار می‌رود که  $aft[\text{break};] = aft[S]$  باشد. اینکه دستورات برنامه پس از اجرای  $\text{break};$  از خارج (یا به عبارت بهتر بعد از) حلقه‌ی  $S$  پی گرفته شود انتظار معقولی است از سیستمی که در حال توصیف رد اجرای برنامه‌های کامپیوتری است. از پس این فرض ما  $aft[\text{break};] = brk - to[S_t]$  نتیجه می‌شود و طبق تعریف معنای دستورات  $\text{break};$  رد پیشوندی زیر در معنای این دستور وجود دارد

$$\langle at[\text{break};], \rho \rangle \langle aft[\text{break};], \rho \rangle$$

که نشانه‌ی توقف است.

◀◀  $S = \{SI''\}$  :

در این صورت توقف پذیری  $SI''$  را از فرض استقرای استقرایی که روی لیست دستورات زده بودیم داریم پس  $\{SI\}$  هم توقف پذیر است. در اینجا اثبات این طرف قضیه به پایان می‌رسد.  
( $\Leftarrow$ )

□

## فصل ۳

# وارسی مدل منظم

در این فصل قرار است به بیانی ساختارمندتر از روش واریسی مدل برسیم. اهمیت ساختارمند تر بودن در این است که بیانی که در فصل پیش داشتیم تا پیاده سازی فاصله‌ی بسیاری دارد، چون همان‌طور که پیش‌تر گفته شد مجموعه‌ها موجودات ساختنی‌ای نیستند و کار با آن‌ها حین نوشتن برنامه‌ای کامپیوتری که قرار است پیاده‌سازی روش مورد بحث ما باشد را سخت می‌کند. ساختاری که در این فصل به صورت روش واریسی مدل اضافه می‌شود، ساختار عبارات منظم است، از این رو پیش از اینکه به بیان واریسی مدل منظم بپردازیم، نیاز داریم که ابتدا به بررسی و تعریف برخی خواص عبارات منظم بپردازیم که در ادامه برای بیان واریسی مدل مورد نیاز هستند.

### ۱.۳ در مورد عبارات منظم

در این بخش ابتدا مفهوم هم‌ارز بودن را برای عبارات منظم تعریف می‌کنیم، سپس به سراغ تعریف دو تابع  $dnf$  و  $fstnxt$  می‌رویم.

#### ۱.۱.۳ هم‌ارزی عبارات منظم

خیلی ساده هم‌ارزی بین دو عبارت منظم را با برابر بودن معنای آن دو تعریف می‌کنیم.

تعریف ۱.۳. (هم‌ارزی عبارات منظم): دو عبارت منظم  $R_1$  و  $R_2$  را هم‌ارز می‌گوییم اگر و تنها اگر شرط زیر برقرار باشد:

$$\mathcal{S}^r[\llbracket R_1 \rrbracket] = \mathcal{S}^r[\llbracket R_2 \rrbracket]$$

این هم‌ارزی را با  $R_1 \approx R_2$  نمایش می‌دهیم.



### ۲.۱.۳ فرم نرمال فصلی

یک دسته از عبارات منظم هستند که به آن‌ها می‌گوییم فرم نرمال فصلی. در صورتی از واریسی مدل که در این فصل ارائه شده، مفهوم فرم نرمال فصلی حضور دارد، بنابراین باید به بحث در مورد آن، پیش از رسیدن به صورت جدید، بپردازیم.

تعریف ۲.۳. (فرم نرمال فصلی): عبارت منظم  $R \in \mathbb{R}$  را یک فرم نرمال فصلی می‌گوییم اگر و تنها اگر با فرض اینکه عبارات منظم بدون انتخاب  $R_1, R_2, \dots, R_n \in \mathbb{R}^+$  وجود داشته باشند که  $R = R_1 + R_2 + \dots + R_n$ .

در تعریف بالا به  $=$  دقت شود که با  $\approx$  که در ادامه مورد بحث ماست فرق می‌کند. به سبک رایج منظور از  $=$  همان تساوی نحوی است.

در ادامه می‌خواهیم یک تابع به اسم  $\text{dnf}$  تعریف کنیم که یک عبارت منظم  $R$  را می‌گیرد و عبارت منظم  $R'$  را تحویل می‌دهد که یک فرم نرمال فصلی است و  $R \approx R'$  برقرار است. ابتدا این تابع را به صورت استقرایی روی ساختار عبارات منظم تعریف می‌کنیم، سپس خاصیتی که گفتیم را در مورد آن ثابت می‌کنیم. این اثبات این حقیقت خواهد بود که هر عبارت منظم با یک فرم نرمال فصلی هم ارز است.

تعریف ۳.۳. (تابع  $\text{dnf}$ ): تابع  $\text{dnf}$  روی عبارات منظم به شکل زیر تعریف می‌شود:

$$\blacktriangleleft \text{dnf}(\varepsilon) = \varepsilon$$

$$\blacktriangleleft \text{dnf}(L : B) = L : B$$

$$\blacktriangleleft \text{dnf}(R_1 R_2) = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} R_1^i R_2^j$$

$$\text{where } R_1^1 + R_1^2 + \dots + R_1^{n_1} = \text{dnf}(R_1) \text{ and } R_2^1 + R_2^2 + \dots + R_2^{n_2} = \text{dnf}(R_2)$$

$$\blacktriangleleft \text{dnf}(R_1 + R_2) = \text{dnf}(R_1) + \text{dnf}(R_2)$$

$$\blacktriangleleft \text{dnf}(R^*) = ((R_1)^*(R_2)^* \dots (R_n)^*)^*$$

$$\text{where } \text{dnf}(R) = R^1 + R^2 + \dots + R^n$$

$$\blacktriangleleft \text{dnf}(R^+) = \text{dnf}(RR^*)$$

$$\blacktriangleleft \text{dnf}((R)) = (\text{dnf}(R))$$

قضیه ۴.۳. اگر  $R \in \mathbb{R}$  آنگاه  $\text{dnf}(R)$  یک ترکیب نرمال فصلی است.

اثبات. همان طور که گفتیم روی ساختار  $R$  استقرا می‌زنیم.

$$\blacktriangleleft R = \varepsilon :$$

$$\text{dnf}(\varepsilon) = \varepsilon$$

که  $\varepsilon$  یک فرم نرمال فصلی است.

$$\blacktriangleleft R = L : B :$$

$$\text{dnf}(L : B) = L : B$$

که  $L : B$  هم یک فرم نرمال فصلی است.

$$\blacktriangleleft R = R_1 R_2 :$$

فرض استقرا این خواهد بود که  $\text{dnf}(R_1) = R_1^1 + R_1^2 + \dots + R_1^n$  و  $\text{dnf}(R_2) = R_2^1 + R_2^2 + \dots + R_2^n$  درحالی‌که  $\text{dnf}(R_1)$  و  $\text{dnf}(R_2)$  ترکیب نرمال فصلی هستند، یعنی هر  $R_1^i$  و هر  $R_2^j$  عضو  $\mathbb{R}^+$  است. طبق تعریف خواهیم داشت:

$$\text{dnf}(R_1 R_2) = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} R_1^i R_2^j$$

که طرف راست عبارت بالا یک ترکیب نرمال فصلی است، چون هر  $R_1^i R_2^j$  یک عضو از  $\mathbb{R}^+$  است.

$$\blacktriangleleft R = R_1 + R_2 :$$

فرض استقرا این خواهد بود که  $\text{dnf}(R_1)$  و  $\text{dnf}(R_2)$  ترکیب فصلی نرمال هستند پس  $\text{dnf}(R_1 + R_2)$  هم که برابر با  $\text{dnf}(R_1) + \text{dnf}(R_2)$  است، ترکیب فصلی نرمال خواهد بود.

$$\blacktriangleleft R = R_1^* :$$

طبق فرض استقرا داریم که  $\text{dnf}(R_1)$  یک ترکیب نرمال فصلی است. همین طور طبق تعریف  $\text{dnf}$  داریم

$$\text{dnf}(R_1^*) = ((R_1^1)^* (R_1^2)^* \dots (R_1^n)^*)$$

که

$$\text{dnf}(R_1) = R_1^1 + R_1^2 + \dots + R_1^n$$

که اینکه  $((R_1^1)^* (R_1^2)^* \dots (R_1^n)^*)$  یک فرم نرمال فصلی است مشخص است چون می‌دانیم در هیچ کدام از این  $R_1^i$  ها عملگر + وجود ندارد و عملگر \* و عملگر چسباندن هم تغییری در این وضع ایجاد نمی‌کنند.

$$\blacktriangleleft R = R_1^+ :$$

طبق چیزهایی که از قبل داریم:

$$\text{dnf}(R_1^+) = \text{dnf}(R_1 R_1^*)$$

$$\text{dnf}(R_1^*) = ((R_1^1)^* (R_1^2)^* \dots (R_1^n)^*)$$

که گیریم  $R' = \text{dnf}(R_1^*)$  که عضو  $\mathbb{R}^+$  است. همین طور فرض می‌کنیم:

$$R_1 = R_1^1 + \dots + R_1^n$$

پس با توجه به تعریف dnf برای عملگر چسباندن خواهیم داشت:

$$\text{dnf}(R_1^+) = \sum_{i=1}^n R_1^i R'$$

$$\blacktriangleleft R = (R_1) :$$

طبق تعریف داریم:

$$\text{dnf}((R_1)) = (\text{dnf}(R_1))$$

طبق فرض استقرا  $\text{dnf}(R_1)$  یک ترکیب نرمال فصلی است، بنابراین  $R' \in \mathbb{R}^+$   $(\text{dnf}(R_1)) = R'$  هم یک ترکیب فصلی نرمال خواهد بود.

□

گزاره‌ی دیگری که برای اثبات مانده برقرار بودن  $R \approx \text{dnf}(R)$  است. برای اثبات آن باید ابتدا قضیه‌ی زیر را اثبات کنیم که اثبات آن را ارجاع می‌دهیم به [۱۳].

قضیه ۵.۳. برای هر دو عبارت منظم  $R_1, R_2 \in \mathbb{R}$  داریم:

$$(R_1 + R_2)^* \approx (R_1^* R_2^*)^*$$

قضیه ۶.۳. برای هر  $R \in \mathbb{R}$  داریم:

$$\text{dnf}(R) \approx R$$

اثبات. طبق این اثبات با استقرا روی ساختار R انجام می‌شود.

$$\blacktriangleright R = \varepsilon :$$

$$\text{dnf}(\varepsilon) = \varepsilon \Rightarrow \mathcal{S}^r[\text{dnf}(\varepsilon)] = \mathcal{S}^r[\varepsilon]$$

►  $R = L : B$  :

$$\text{dnf}(L : B) = L : B \Rightarrow \mathcal{S}^r[\text{dnf}(L : B)] = \mathcal{S}^r[L : B]$$

►  $R = R_1 R_2$  :

برای اثبات این حالت باید دو عبارت زیر را ثابت کنیم:

$$\mathcal{S}^r[R_1 R_2] \subseteq \mathcal{S}^r[\text{dnf}(R_1 R_2)]$$

$$\mathcal{S}^r[R_1 R_2] \supseteq \mathcal{S}^r[\text{dnf}(R_1 R_2)]$$

فرض می‌کنیم  $\langle \underline{\rho}, \pi \rangle$  یک عضو دلخواه از  $\mathcal{S}^r[\text{dnf}(R_1 R_2)]$  باشد. چون  $\text{dnf}(R_1 R_2) = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} R_1^i R_2^j$  پس داریم:

$$\exists k_1, k_2 : \pi \in \mathcal{S}^r[R_1^{k_1} R_2^{k_2}]$$

$$\Rightarrow \exists \pi_1, \pi_2 \text{ s.t. } \pi = \pi_1 \pi_2, \langle \underline{\rho}, \pi_1 \rangle \in \mathcal{S}^r[R_1^{k_1}], \langle \underline{\rho}, \pi_2 \rangle \in \mathcal{S}^r[R_2^{k_2}]$$

با این وجود داریم:

$$\mathcal{S}^r[R_1^{k_1}] \subseteq \mathcal{S}^r[R_1], \mathcal{S}^r[R_2^{k_2}] \subseteq \mathcal{S}^r[R_2]$$

$$\Rightarrow \langle \underline{\rho}, \pi_1 \pi_2 \rangle = \langle \underline{\rho}, \pi \rangle \in \mathcal{S}^r[R_1 R_2]$$

: ( $\subseteq$ )

$$\langle \underline{\rho}, \pi \rangle \in \mathcal{S}^r[R_1 R_2]$$

$$\Rightarrow \exists \pi_1, \pi_2 : \pi = \pi_1 \pi_2 \text{ s.t. } \langle \underline{\rho}, \pi_1 \rangle \in \mathcal{S}^r[R_1], \langle \underline{\rho}, \pi_2 \rangle \in \mathcal{S}^r[R_2]$$

طبق فرض استقرا داریم:

$$\mathcal{S}^r[R_1] = \mathcal{S}^r[\text{dnf}(R_1)], \mathcal{S}^r[R_2] = \mathcal{S}^r[\text{dnf}(R_2)],$$

$$\Rightarrow \exists k_1, k_2 : \langle \underline{\rho}, \pi_1 \rangle \in \mathcal{S}^r[R_1^{k_1}], \langle \underline{\rho}, \pi_2 \rangle \in \mathcal{S}^r[R_2^{k_2}]$$

$$\Rightarrow \langle \underline{\rho}, \pi \rangle \in \mathcal{S}^r[R_1^{k_1} R_2^{k_2}] \subseteq \mathcal{S}^r[\text{dnf}(R_1 R_2)]$$

□

## فصل ۴

### وارسی مدل ساختارمند

## فصل ۵

### نتیجه گیری

## واژه‌نامه فارسی به انگلیسی

## واژه‌نامه انگلیسی به فارسی



# Bibliography

- [1] Committee to review chinook zd 576 crash. report from the select committee on chinook zd 576., Feb 2002.
- [2] A. S. E. Al. Mars climate orbiter mishap investigation board phase i report., November 1999.
- [3] A. Chlipala. *Certified Programming with Dependent Types: A Pragmatic Introduction to Coq Proof Assistant*. MIT Press, 2022.
- [4] E. M. Clarke and E. A. Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. In D. Kozen, editor, *Logic of Programs*, volume 131 of *Lecture Notes in Computer Science*, pages 52–71. Springer, 1981.
- [5] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model checking*. MIT Press, London, Cambridge, 1999.
- [6] P. Cousot. Calculational design of a regular model checker by abstract interpretation. In R. M. Hierons and M. Mosbah, editors, *ICTAC*, volume 11884 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 2019.
- [7] P. Cousot. *Principals of Abstract Interpretation*. MIT Press, 2021.
- [8] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *POPL '77: Proceedings of the 4th ACM SIGACT-SIGPLAN symposium on Principles of programming languages*, pages 238–252. ACM Press, 1977.
- [9] M. Davis and E. Weyuker. *Computability, Complexity, and Languages*. Academic Press, New York, 1983.

- [10] D. Harel, D. Kozen, and J. Tiuryn. Dynamic logic. In *Handbook of philosophical logic*, pages 99–217. Springer, 2001.
- [11] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 1969.
- [12] M. Huth and M. Ryan. *Logic in computer science : modelling and reasoning about systems*. Cambridge University Press, Cambridge [U.K.]; New York, 2004.
- [13] R. M. John E. Hopcroft and J. D. Ullman. Introduction to automata theory, languages, and computation. page 118, 2003.
- [14] X. R. K. Yi. *Introduction to Static Analysis: An Abstract Interpretation Perspective*. MIT Press, 2020.
- [15] S. Kleene. Representation of Events in Nerve Nets and Finite Automata. In C. Shannon and J. McCarthy, editors, *Automata Studies*, pages 3–41. Princeton University Press, 1956.
- [16] S. A. Kripke. A completeness theorem in modal logic<sup>1</sup>. *The journal of symbolic logic*, 24(1):1–14, 1959.
- [17] J. Lions. Ariane 5 Flight 501 Failure: Report of the Inquiry Board, July 1996.
- [18] M. Mukund. Linear-time temporal logic and buchi automata. *Tutorial talk, Winter School on Logic and Computer Science, Indian Statistical Institute, Calcutta*, 1997.
- [19] G. J. Myers, C. Sandler, and T. Badgett. *The art of software testing*. John Wiley & Sons, Hoboken and N.J, 3rd ed edition, 2012.
- [20] B. C. Pierce, A. Azevedo de Amorim and Chris Casinghino, M. Gaboardi, M. Greenberg, C. Hrițcu, V. Sjöberg, A. Tolmach, and B. Yorgey. *Programming Language Foundations*. Software Foundations series, volume 2. Electronic textbook, May 2018.
- [21] H. G. Rice. Classes of recursively enumerable sets and their decision problems. *Transactions of the American Mathematical Society*, 74(2):358–366, 1953.

- [22] A. Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific journal of Mathematics*, 5(2):285–309, 1955.
- [23] G. Winskel. *The formal semantics of programming languages - an introduction*. Foundation of computing series. MIT Press, 1993.
- [24] P. Wolper. Temporal logic can be more expressive. *Inf. Control.*, 56(1/2):72–99, January/February 1983.

## **Abstract**

Abstract goes here...



College of Science  
School of Mathematics, Statistics, and Computer Science

# Thesis Title

## **Author name**

Supervisor: name  
Co-Supervisor: name  
Advisor: name

A thesis submitted to Graduate Studies Office  
in partial fulfillment of the requirements for the degree of  
B.Sc./Master of Science/Doctor of Philosophy in  
Pure Mathematics/ Applied Mathematics/ Statistics/ Computer Science

yyyy