وزارت علوم، تحقیقات و فناوری
دانشگاه دامغان
دانشکده ریاضی و علوم کامپیوتر

پایان‌نامه کارشناسی ارشد
ریاضی محض

درستی‌یابی گمنامی در منطق شناختی

توسط:
حسین کلاته سیفری

استاد راهنما:
دکتر مصطفی زارع خورمیزی

استاد مشاور:
دکتر بهزاد صالحیان

شهریور ۱۳۹۱


بسم الله الرحمن الرحيم

به نام خدا

درستی‌یابی گمنامی در منطق شناختی

توسط:

حسین کلاته سیفری

پایان‌نامه

ارائه شده به تحصیلات تکمیلی دانشگاه به عنوان بخشی از فعالیت‌های
تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته

ریاضی محض

از دانشگاه دامغان

ارزیابی و تأیید شده توسط کمیته پایان‌نامه با درجه: **بسیار خوب**

دکتر مصطفی زارع خورمیزی استادیار ریاضی محض گرایش منطق ریاضی دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان (استاد راهنما)

دکتر بهزاد صالحیان متی‌کلایی استادیار ریاضی محض گرایش گراف و ترکیبیات دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان (استاد مشاور)

دکتر مجتبی آقایی استادیار ریاضی محض گرایش منطق ریاضی دانشکده علوم ریاضی دانشگاه صنعتی اصفهان (داور اول)

دکتر مجید فرهادی استادیار ریاضی محض گرایش هندسه جبری دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان (داور دوم)

دکتر سید هاشم طبسی استادیار علوم کامپیوتر دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان (نماینده تحصیلات تکمیلی)

شهریور ۱۳۹۱

تقدیم به

منجی عالم بشریت حضرت مهدی (عج)

و پدر و مادر بزرگوارم

و همسر و فرزندانم مینا و محمد

سپاسگزاری

ستایش مخصوص خداوندی است که هیچ گوینده و سخنوری توانایی ستودن او را بدان گونه که شایسته ذات مقدس اوست ندارد، هیچ حساب گری قادر به شماردن نعمت های او نیست و سخت کوشان جهان هر قدر بکوشند، به ادای حق او توانا نیستند.

خداوندی که صاحبان همت های بلند و متفکران دوراندیش، قدرت درک او را اندازند و زیرکی های بشری، هر اندازه در دریای معقولات برای کشف حقیقت ذات او غوطه ور شوند، بدان نمی رسند.

از استاد گرانقدرم جناب آقای دکتر مصطفی زارع به خاطر راهنمایی های ارزشمندشان در طول انجام این پایان نامه و همچنین از استاد ارجمندم جناب آقای دکتر بهزاد صالحیان که زحمت مشاوره این پایان نامه را تقبل فرمودند، صمیمانه سپاس گزارم.

از اساتید بزرگوار جناب آقای دکتر مجتبی آقایی و جناب آقای دکتر مجید فرهادی که در مقام داور زحمت مطالعه پایان نامه را بر عهده داشتند و از نماینده تحصیلات تکمیلی جناب آقای دکتر سید هاشم طبسی قدردانی می نمایم.

آخرین، امانه کمترین: از همسرم و فرزندانم، که در دوران نگارش این پایان نامه با صبر و شکیبایی مرا از بعضی کارهای منزل معاف می کردند، بسیار سپاس گزارم.

چکیده

درستی‌یابی گمنامی در منطق شناختی

به وسیله‌ی:
حسین کلاته سیفری

گمنامی خاصیتی قابل ردیابی نیست، از این رو بررسی‌گرهای مدل سنتی توانایی بیان و درستی‌یابی آن را ندارند. از طرف دیگر با بهره‌گیری از منطق شناختی برای مدل کردن پروتکل‌ها، می‌توان گمنامی را با فرمولی شناختی بیان و درستی‌یابی کرد. در این پایان‌نامه هدف استفاده از منطق شناختی پویا برای مدل‌سازی پروتکل‌های امنیت و خاصیت‌ها به ویژه خاصیت گمنامی است. در انتها به مقایسه مدل‌سازی منطق شناختی پویا و مدل‌سازی فرآیند می‌پردازیم و محاسن و معایب هر روش را بررسی می‌کنیم.

واژه‌های کلیدی: منطق شناختی، مدل‌سازی شناختی پویا، درستی‌یابی پروتکل، گمنامی.

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

پیش‌گفتار

تفکر و اندیشه همانند نطق و سخن گفتن است. همان‌گونه که نطق و سخن گفتن را انسان فطرتا می‌داند، اما برای تصحیح و استوارسازی آن نیازمند قواعد و قوانینی است که "دستور زبان" خوانده می‌شود، همچنین اصل تفکر و اندیشه را انسان فطرتا می‌داند، اما برای تصحیح و درست سازی آن نیازمند قوانین و قواعدی است، که شیوه صحیح تفکر را به انسان تعلیم دهد. مجموعه این قوانین، منطق نامیده می‌شود. پس انسان برای تصحیح افکار خویش نیازمند به "منطق" است.

از این رو در تعریف منطق آورده‌اند: "منطق ابزاری از جنس قانون است که رعایت کردن آن موجب می‌شود ذهن از خطا در اندیشه مصون بماند."

این تعریف، تعریف قدما می‌باشد که منطق را یک آلت برای تصحیح فکر می‌دانستند و به همین دلیل، منطق یک علم آلی بود. یعنی ابزاری است در خدمت دیگر علوم، و خود به تنهایی پرده از حقایق خارج بر نمی‌گیرد. و برای مصون ماندن از خطا در تفکر و اندیشه، فراگیری قوانین منطق به تنهایی کفایت نمی‌کند، بلکه باید علاوه بر آن، این قوانین را به کار برد و رعایت نمود.

متاخرین نیز، با تعابیر مختلف، منطق را علم استدلال و منطق ریاضی را علم استدلال ریاضی می دانند. هیتینگ [1] منطق ریاضی را مدل سازی ریاضی تفکر ریاضی می‌داند.

منطق ریاضی شامل انواع منطق کلاسیک، منطق شهودگرایانه، منطق موجهات، منطق شناختی [2]، منطق خطی، منطق چند ارزشی، منطق فقه یا تکلیف، منطق زمان و منطق فازی می‌باشد.

منطق مورد بحث در این پایان‌نامه منطق شناختی است. منطق شناختی زبان صوری برای توصیف آگاهی‌های هر عامل در یک سیستم چندعاملی فراهم می‌کند. این منطق مفاهیم توافق چند عامل بر

[1] A.Heyting

[2] Epistemic Logic

سر یک موضوع و آگاهی توزیع شده بین عامل‌ها را نیز به خوبی مدل می‌کند. منطق اعلان عمومی [۳] و منطق عمل شناختی [۴] توسیع‌های دینامیکی از منطق شناختی هستند که به توصیف کردن به روز رسانی [۵] آگاهی‌ها در یک سیستم چند عاملی [۶] می‌پردازند. دونوع به روزرسانی آگاهی را برای یک سیستم چند عاملی می‌توان در نظر گرفت.

- به روزرسانی که یک آگاهی، در حضور همه عامل‌ها، به اطلاع همه عامل‌های سیستم می‌رسد. این نوع به روزرسانی آگاهی را اعلان عمومی می‌گوییم. منطق اعلان عمومی برای توصیف و استنتاج در مورد این نوع به روزرسانی کاراست.
- به روزرسانی که یک آگاهی فقط به یک زیرگروه از عامل‌ها اعلان می‌شود. این نوع به روزرسانی آگاهی را اعلان خصوصی [۷] می‌نامیم. منطق عمل شناختی برای مدل کردن به روزرسانی نوع دوم کاراست.

یک پروتکل یا یک الگوریتم چند عاملی عبارت است از مشخص کردن این که هر عامل باید چه عملی را انجام دهد تا هدف مورد نظر برای سیستم اجتماعی [۸] برآورده شود. باید دقت کرد که در یک سیستم اجتماعی هر عاملی به دنبال اهداف خود است و یک پروتکل با توجه به این موضوع باید طراحی شود. گمنامی [۹] یا گمنام ماندن یکی از مسائل مهم در بسیاری از پروتکل‌هاست. نمونه‌های بسیاری از این پروتکل‌ها وجود دارد، مثلاً رأی گیری الکترونیکی، جستجو در وب، به اشتراک‌گذاری فایل‌ها [۱۰] و انواعی از مناقصه‌ها از این دسته‌اند. برای نمونه یک رأی گیری را در نظر بگیرید، در بسیاری از موارد افراد دوست دارند رأیشان به دلایلی مخفی بماند. از طرف دیگر افراد دیگری نیز به دلایلی خواهان به دست آوردن هویت صاحبان این رأی‌ها هستند. با توجه به این موارد و هدف که برگزاری انتخابات با رأی مخفی است، باید روش‌هایی را به کار بریم که ناشناس ماندن رأی دهندگان تضمین گردد. پرسشی که اکنون مطرح می‌گردد این است که چگونه از درستی روش خود اطمینان حاصل کنیم؟ به سخن دیگر چگونه بفهمیم روش ما امکانی برای افراد متخلف فراهم نمی‌کند تا به رأی دیگران دسترسی پیدا کنند؟ معمولاً در چنین مواردی دوست داریم بتوانیم خاصیت مورد بررسی را در یک چارچوب استنتاجی و به

[۳] Public Announcement

[۴] Epistemic Action

[۵] Update

[۶] Multi - agent system

[۷] Private announcement

[۸] Social system

[۹] Anonymity

[۱۰] Sharing files

وسیله‌ی نرم افزارها بررسی کنیم. اما متأسفانه در مورد گمنامی چنین رویکردی چندان راحت نیست. مشکل این جاست که تعریف گمنامی در اکثر چارچوب‌های خوبی که تا به حال ساخته شده‌اند امکان پذیر نیست. در واقع خاصیتی مانند گمنامی نسبت به خواص دیگر امنیتی مانند سری بودن پیچیدگی بیش‌تری دارد و به علاوه گمنامی وابسته به شخص است، یعنی با توجه به هر فرد نامعتمد خارجی باید دوباره جهان را مدل کرد. هر دو مشکل آمده در بالا با استفاده از روش‌های مبتنی بر منطق شناختی قابل حل است.

نکته مهم در این روش جدید توجه ما به جریان اطلاعات است نه بر رفتارهای مشاهده گرها. در واقع یک حالت شناختی [۱۱] از یک پروتکل در بردارنده تمام اطلاعات و عدم قطعیت‌های تمام طرف‌ها از واقعیت موجود است. گمنامی یک عامل را می‌توان عدم قطعیت یک ناظر خاص نسبت به یک گزاره مشخص، که درواقع مدلی است از اطلاعات حساس آن عامل، دانست. چنین گزاره‌ای در منطق شناختی به راحتی قابل نشان دادن است. البته باید دانست در حالت کلی نشان دادن گمنامی در پروتکل‌ها و هم‌چنین بررسی روزآمد شدن اطلاعات می‌تواند بسیار پیچیده باشد و به مهارت بسیار نیاز دارد.

در این پایان‌نامه، به بررسی منطق شناختی پویا [۱۲] (DEL) برای تحقیق خودکار گمنامی می‌پردازیم. منطق شناختی پویا روزآمدی اطلاعات را نسبت به انواع مختلف ارتباط (اعلان عمومی، انتقال پیام [۱۳]، اشتراک رازها [۱۴]، دروغ گفتن [۱۵]) توصیف می‌کند. درواقع مزیت کار با این منطق در این است که هم توان و عملکرد قوی‌ای دارد و هم از قابلیت ذاتی نمایش رفتارها به شکل تصویری برخوردار است. چنین خصوصیاتی این منطق را از هر لحاظ برای کار پروتکل‌های امنیتی مناسب می‌کند.

با توجه به نحوه اثبات در منطق شناختی که در ساختار مدل کریپکی [۱۶] شکل می‌گیرد، به نظر می‌رسد در صورتی که بتوانیم از نرم افزاری برای رسم تمام مدل‌های کریپکی و رسیدن به حالت نهایی دانش استفاده کنیم، می‌توانیم مسائلی مانند بررسی پروتکل‌های امنیتی را به راحتی و به سرعت حل کنیم. یکی از این نرم افزارها به نام $CADP$ برای چک کردن مدل‌ها و یک مجموعه ابزار کمکی به نام μCRL و همچنین یک برنامه کمکی دیگر برای کشیدن گرافیکی مدل‌ها به نام LYS استفاده می شود.

---

[۱۱] Epistemic state

[۱۲] Dynamic Epistemic Logic

[۱۳] Passing message

[۱۴] Sharing secrets

[۱۵] Telling lies

[۱۶] Kripke model

ساختار پایان‌نامه به شرح زیر است:

در فصل اول به معرفی منطق شناختی می‌پردازیم. در این فصل زبان منطق شناختی، مدل‌های کریپکی و اصول منطق شناختی را معرفی می‌کنیم و با ارائه مثال‌های نسبتاً ساده مفاهیم معرفی شده را توضیح می‌دهیم. در فصل دوم، منطق‌های شناختی پویا را معرفی می‌کنیم. در ابتدا منطق اعلان عمومی و سپس منطق عمل شناختی را معرفی می‌کنیم. در این فصل نیز از آوردن مثال کوتاهی نمی‌کنیم.

در فصل سوم، به شرح مفهوم درستی‌یابی، بررسی گرهای مدل و ویژگی گمنامی می‌پردازیم. پروتکل شام رمزنگارها و پروتکل رأی‌گیری الکترونیکی FOO را از دو منظر بیان می‌کنیم، گمنامی نیاز اساسی این پروتکل‌ها می‌باشد، که درپروتکل‌های ارائه شده این نیاز برطرف می‌شود، در این‌جا ما به اثبات گمنامی و چند فرمول دیگر در پروتکل شام رمزنگارها می‌پردازیم. همچنین به یک مقایسه اجمالی بین مدل‌سازی DEL و مدل‌سازی فرآیند در پروتکل DC می‌پردازیم.

فصل ۱

منطق شناختی

۱-۱ زبان و گرامر منطق شناختی

منطق شناختی زبانی صوری برای توصیف و تحلیل دانش [۱] یا باور [۲] عامل‌ها فراهم می‌کند. فرض کنید سه کارت قرمز، سفید و آبی به ترتیب بین سه بازیکن ۱، ۲ و ۳ توزیع شده‌اند. بازیکنان تنها کارت خویش را می‌بینند و همگی می‌دانند که کارت‌ها به گونه‌ای میان آن‌ها توزیع شده است. به وسیله‌ی منطق شناختی می‌توان جملات پیچیده‌ای را مانند "بازیکن ۲ می‌داند که بازیکن ۱ نمی‌داند چه کارتی دست بازیکن ۳ است." صوری کرد. حتی علم به این که دقیقاً سه کارت وجود دارد و علم به رنگ کارت‌ها را که یک همه دانی مشترک است می‌توان فرمول‌بندی کرد.

تعریف ۱.۱.۱. فرض کنید P مجموعه‌ی گزاره‌های اتمی سیستم و A مجموعه‌ی عامل‌های سیستم باشد. زبان منطق شناختی $\mathcal{L}_{EL}$ کوچکترین مجموعه‌ای است که شرایط زیر را داشته باشد:

- اگر $p \in P$ آنگاه $p \in \mathcal{L}_{EL}$،
- اگر $\varphi, \psi \in \mathcal{L}_{EL}$ آنگاه $\neg\varphi, (\varphi \wedge \psi) \in \mathcal{L}_{EL}$،
- اگر $\varphi \in \mathcal{L}_{EL}$ آنگاه برای هر $a \in A$، $\Box_a\varphi \in \mathcal{L}_{EL}$.

[۱] Knowledge

[۲] Belief

نماد $\neg$ و $\wedge$ معمولاً عملگرهای بولی اطلاق می‌شوند و $\Box_a$ برای هر $a \in A$ عملگرهای شناختی نامیده می‌شوند. برای هر عامل $a \in A$، فرمول $\Box_a\varphi$ به صورت‌های "عامل a، φ را می‌داند." و یا "عامل a، φ را باور دارد." خوانده می‌شود.
توجه کنید که ادوات $\vee$، $\rightarrow$ و $\leftrightarrow$ با توجه به خلاصه نویسی‌های زیر از ادوات $\neg$ و $\wedge$ به دست می‌آیند:

- $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$،
- $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$،
- $\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

و فرمول $\top$ (همیشه درست) از خلاصه نویسی $\top \equiv p \vee \neg p$ که p یک گزاره اتمی دلخواه است و فرمول $\bot$ (همیشه غلط) از خلاصه نویسی $\bot \equiv \neg\top$ به دست می‌آید.

۱-۲ معناشناسی منطق شناختی

در بخش قبل به این پرداختیم که چگونه به وسیله‌ی گزاره‌های اتمی سیستم می‌توان گزاره‌های مرکب ساخت. اکنون می‌خواهیم در مورد مفهوم درستی یک گزاره و این که یک گزاره در چه شرایطی صادق است صحبت کنیم. درستی یک گزاره φ، مربوط به یک سیستم چند عاملی، در مدل کریپکی دانش آن سیستم چند عاملی مشخص می‌شود.

تعریف ۱.۲.۱. فرض کنید P مجموعه‌ی شمارای گزاره‌های اتمی و A یک مجموعه متناهی از عامل‌ها باشد. یک مدل کریپکی یک سه‌تایی

$$M = \langle S, (R_a)_{a\in A}, V\rangle$$

است به طوری که

- S مجموعه همه حالت‌های ممکن سیستم (جهان‌های ممکن) است و $S = \mathcal{D}(M)$،
- برای هر عامل $a \in A$، $R_a \subseteq S \times S$ رابطه ای بین حالت‌ها است که مشخص می‌کند عامل a با توجه به میزان دسترسی‌اش به اطلاعات سیستم، چه حالت‌هایی را نمی‌تواند از هم تمیز دهد،
- $V : P \rightarrow ۲^S$ که به هر گزاره‌ی اتمی یک زیرمجموعه از S را نسبت می‌دهد برای هر $p \in P$، $V(p) \subseteq S$ حالت‌هایی است که p در آن‌ها درست می‌باشد.

معمولاً sR_at را به صورت R_ast نمایش می‌دهیم. اگر همه رابطه‌های R_a در M رابطه‌های هم ارزی باشند، مدل کریپکی M یک مدل شناختی نامیده می‌شود و رابطه‌ی R_a را به صورت $\sim_a$ می‌نویسیم و مدل شناختی را به صورت $M = \langle S, \sim, V\rangle$ نمایش می‌دهیم. کلاس مدل‌های کریپکی با روابط هم ارزی را با $S5$ نشان می‌دهیم.

تعریف ۲.۲.۱. برای هر $s \in S$، زوج (M, s) را یک مدل نقطه‌ای [۳] (یک جهان ممکن) در مدل M می‌نامیم. ارضا شدن [۴] (راست بودن) یک گزاره $\varphi \in \mathcal{L}_{EL}$ در مدل نقطه‌ای (M, s) با نماد $(M, s) \vDash \varphi$ یا $M \vDash_s \varphi$ نمایش داده می‌شود، و $(M, s) \nvDash \varphi$ یعنی φ در جهان s از مدل M راست نیست. با توجه به ساختار φ، ارضا شدن آن به صورت زیر تعریف می‌گردد:

- $(M, s) \vDash \top$ برای هر $s \in S$،
- $(M, s) \nvDash \bot$ برای هر $s \in S$،
- $(M, s) \vDash p$ اگرو فقط اگر $s \in V(p)$،
- $(M, s) \vDash \neg\varphi$ اگرو فقط اگر $(M, s) \nvDash \varphi$،
- $(M, s) \vDash \varphi \wedge \psi$ اگرو فقط اگر $(M, s) \vDash \varphi$ و $(M, s) \vDash \psi$،
- $(M, s) \vDash \Box_a\varphi$ اگرو فقط اگر $(M, t) \vDash \varphi$ برای هر t که R_ast.

در زبان $\mathcal{L}_{EL}$ خلاصه نویسی زیر را داریم:

$$\Diamond_a\varphi \equiv \neg\Box_a\neg\varphi \equiv \Box_a(\varphi \to \bot) \to \bot$$

با توجه به معناشناسی $\Box_a\varphi$، می‌توان به راحتی نشان داد که: $(M, s) \vDash \Diamond_a\varphi$ اگرو تنها اگر وجود داشته باشد یک t که R_ast و $(M, t) \vDash \varphi$.

اگر برای هر $s \in S$، $(M, s) \vDash \varphi$، می‌نویسیم $M \vDash \varphi$ و می‌گوییم φ در مدل M معتبر [۵] است. اگر φ در کلاس مدل‌های کریپکی، $\mathbb{k}$ درست باشد می‌نویسیم $\mathbb{k} \vDash \varphi$ و اگر در تمام مدل‌های شناختی درست باشد می‌نویسیم $S5 \vDash \varphi$.

تعریف ۳.۲.۱. فرض کنید R رابطه‌ای روی W باشد

---

[۳] Poited model

[۴] Satisfication

[۵] Valid

۱. R بازتابی است اگر برای هر $w \in W$، wRw،

۲. R متقارن است اگر برای هر $w, x \in W$، اگر wRx آنگاه xRw،

۳. R متعدی است اگر برای هر $w, x, y \in W$، اگر wRx و xRy آنگاه wRy،

۴. R سریالی [۶] است اگر برای هر $w \in W$، وجود داشته باشد $x \in W$ به طوری که wRx،

۵. R اقلیدسی [۷] است اگر برای هر $w, x, y \in W$، اگر wRx و wRy آنگاه xRy،

۶. R هم ارزی است اگر R، بازتابی، متقارن و متعدی باشد.

توجه کنید رابطه هم ارزی معادل با این است که رابطه خاصیت بازتابی، اقلیدسی و تعدی داشته باشد.

معمولاً به ازای $a \in A$، $K_a\varphi$ را به جای $\Box_a\varphi$ به کار می‌بریم و $\widehat{K}_a\varphi$ را به جای $\Diamond_a\varphi$ استفاده می‌کنیم یعنی، $\widehat{K}_a\varphi \equiv \neg K_a\neg\varphi$. می‌توانیم $\widehat{K}_a\varphi$ را به صورت "a، φ را ممکن می‌داند" بخوانیم.

مثال ۴.۲.۱. علی از سه کارت مختلف ۰ ، ۱ و۲ که در قفسه هستند کارت ۰ را بیرون می‌کشد. او هنوز کارت خود را ندیده است. کارت ۱ و ۲ به پشت و به ترتیب در قفسه و روی میز قرار داده می‌شوند. علی اکنون کارت خود را می‌بیند. اگر عامل علی را با a و i_a، i_t و i_s برای $i = ۰, ۱, ۲$ به ترتیب بیانگر "کارت i دست علی است"، "کارت i روی میز است" و "کارت i در قفسه است" باشد فرمول عبارت‌های زیر را بیان می‌کنیم:

۱. کارت ۰ دست علی است: ۰_a

۲. علی می‌داند کارت دست او ۰ است: $K_a ۰_a$

۳. علی نمی‌داند کارت ۱ روی میز است: $\neg K_a ۱_t$

۴. علی ممکن می‌داند کارت ۱ روی میز نیست: $\widehat{K}_a \neg ۱_t$

۵. علی می‌داند کارت ۱ یا کارت ۲ در قفسه است: $K_a(۱_s \vee ۲_s)$

۶. علی کارت خودش را می‌داند: $K_a ۰_a \vee K_a ۱_a \vee K_a ۲_a$

---

[۶] Serial

[۷] Euclidean

مثال ۵.۲.۱. علی (a) و بابک (b) روبروی یکدیگر نشسته‌اند. روی پیشانی آن‌ها دو عدد طبیعی متوالی نوشته شده است و از این موضوع هر دو اطلاع دارند و آن‌ها می‌دانند که آن‌ها این مطلب را می‌دانند و . . . . فرض کنیم بر پیشانی علی عدد ۳ $(a_۳)$ و بر پیشانی بابک عدد ۲ $(b_۲)$ نوشته شده باشد. فرمول‌های زیر درست می‌باشند:

۱. $K_b a_۳$ و $K_a b_۲$

۲. $K_b(b_۲ \vee b_۴)$ و $K_a(a_۱ \vee a_۳)$

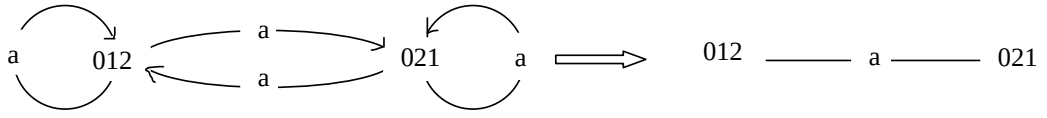
۳. $K_b K_a(a_۱ \vee a_۳ \vee a_۵)$ و $K_a K_b(b_۰ \vee b_۲ \vee b_۴)$

۴. $K_b K_a K_b(a_۱ \vee a_۳ \vee a_۵)$ و $K_a K_b K_a(b_۰ \vee b_۲ \vee b_۴)$

۵. $\widehat{K}_b b_۲ \wedge \widehat{K}_a b_۴$ و $\widehat{K}_a a_۱ \wedge \widehat{K}_a a_۳$

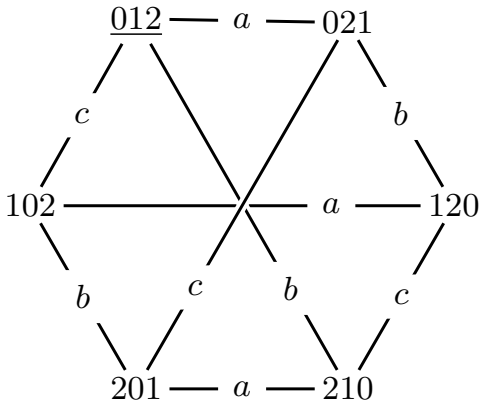
۶. $K_a(\neg win_a \wedge \neg win_b)$، که در آن "علی عدد پیشانی اش را می‌داند" $:= win_a$ و win_b نیز به طور مشابه معرفی می‌شود. دقت شود اگر عدد پیشانی بابک صفر باشد این فرمول درست نیست، زیرا در این صورت علی عدد پیشانی خود را می‌داند. فرمول $K_b(\neg win_a \wedge \neg win_b)$ نیز درست است. ■

برای رسم گراف مدل کریپکی دانش، ابتدا باید برای هر حالت ممکن سیستم یک گره در نظر گرفت. سپس با توجه به میزان دسترسی به اطلاعات هر عامل، یال‌های مربوط به آن عامل را رسم کرد. توجه کنید هر عامل هر حالت را نمی‌تواند از خود آن حالت تمیز دهد و در هر گره برای هر عامل یک طوق با برچسب آن عامل وجود دارد که برای شلوغ نشدن گراف از ترسیم طوق‌ها صرف نظر می‌کنیم. همچنین در صورت وجود یک یال بین دو حالت ممکن و داشتن خاصیت تقارنی دو یال جهت دار باید رسم شود که برای شلوغ نشدن یک یال بدون جهت بین دو حالت رسم می‌کنیم.



مثال ۶.۲.۱. سه کارت ۰، ۱ و ۲ بین سه عامل a، b و c توزیع شده است. به طوری که هر عامل تنها کارت خود را می‌بیند. هر سه عامل عالم به توزیع چنین کارت‌هایی هستند و هر عامل می‌داند که عامل دیگری این را می‌داند و . . . .
مدل کریپکی آن را رسم می‌کنیم و درستی یک فرمول را در جهان واقع نشان می‌دهیم. فرض کنید حالت

واقع ۰۱۲ باشد که این مطلب را با کشیدن یک خط زیر آن نشان داده‌ایم (۰ دست عامل a و ۱ دست عامل b و ۲ دست عامل c است).



- $M = \langle S, \sim, V \rangle$
- $A = \{a, b, c\}$ مجموعه عامل‌ها،
- $S = \{۰۱۲, ۰۲۱, ۱۰۲, ۱۲۰, ۲۰۱, ۲۱۰\}$ مجموعه حالت‌ها،
- $P = \{x_i \mid x = ۰, ۱, ۲ ; i = a, b, c\}$ مجموعه گزاره‌های اتمی است، به طوری که "کارت x دست عامل i است." $:= x_i$،
- $\sim_a = \{(۰۱۲, ۰۱۲), (۰۱۲, ۰۲۱), \ldots\}$ و $\cdots$
- $V(۰_a) = \{۰۱۲, ۰۲۱\}$ و $V(۱_a) = \{۱۰۲, ۱۲۰\}$ و $\cdots$

داریم

$$
\begin{aligned}
&(M, ۰۱۲) \models \widehat{K}_a \widehat{K}_b K_c \neg ۰_a \\
&\Leftarrow ۰۱۲ \sim_a ۰۲۱, (M, ۰۲۱) \models \widehat{K}_b K_c \neg ۰_a \\
&\Leftarrow ۰۲۱ \sim_b ۱۲۰, (M, ۱۲۰) \models K_c \neg ۰_a \\
&\Leftrightarrow \sim_c (۱۲۰) = \{۱۲۰, ۲۱۰\}, (M, ۱۲۰) \models \neg ۰_a, (M, ۲۱۰) \models \neg ۰_a \\
&\Leftrightarrow (M, ۱۲۰) \not\models ۰_a, (M, ۲۱۰) \not\models ۰_a \\
&\Leftrightarrow ۱۲۰, ۲۱۰ \notin V(۰_a) = \{۰۱۲, ۰۲۱\}
\end{aligned}
$$

■