

(آشنایی کوتاه با)

مدل سازی منطقی سیستم های اجتماعی

(آگاهی، تعامل، ائتلاف، تعهد، همزمانی)

(منطق شناختی، منطق بازی، منطق تکلیف، منطق زمانی)

رسول رمضانیان

جزوه درس نظریه سیستم ها

(پیش نویس ۱۳۸۸)

دانشکده علوم ریاضی

دانشگاه صنعتی شریف



A short introduction to

Logical Modeling of Social Systems

(Knowledge, Interaction, Coalition, Obligation, Concurrency)

(Epistemic Logic, Game Logic, Deontic Logic, Temporal Logic)

Rasool Ramezani

Systems Theory Course

Sharif University of Technology

Department of Mathematical Sciences

(DRAFT 2009)

دانشجویان عزیز،

نوشته‌ای که در پیش رو دارید یک پیش‌نویس از **جزوه** درس نظریه سیستم‌ها است که از خطا و اشتباه تهی نیست. خواهشمندم با پیدا کردن و گزارش این خطاها، در بهبود جزوه همکاری کنید. این جزوه همواره ناقص خواهد بود و کامل‌تر^۱ شدن آن بدون یاری شما ممکن نیست.

با سپاس فراوان

رسول رمضانیان

^۱ آنچه کاملترین است نقصش این است که نمی‌تواند خود را کامل‌تر کند.

فهرست

مقدمه

بخش اول: علوم اجتماعی

۱- آشنایی کوتاه با نظریه‌های علوم اجتماعی (برای نوشتن این قسمت مطالعاتم کافی و اندیشه‌هایم منسجم نیست. اما

حتما این فصل را خواهم نوشت)

۱-۱ کنترل اجتماعی

۱-۲ عقلانیت (سودجویی) فردی^۲ در برابر اخلاق جمعی (هر آنچه برای خود می‌پسندی برای

دیگران بپسند)

۱-۳ تبعیت از جمع و دانش توزیع شده ناسازگار

۱-۴ باور مشترک نادرست

.....

۲- سیستم‌های اجتماعی (چندعاملی)

۲-۱ آگاهی

۲-۲ تعامل

۲-۳ ائتلاف

۲-۴ تعهد

۲-۵ همزمانی

۶-۲ تکامل

۷-۲ خودتنظیمی

۸-۲ نیازها

تمرین‌ها

مراجع

بخش دوم: مدل‌سازی منطقی

۳- مروری کوتاه بر منطق گزاره‌ای و منطق محمولات

۱-۳ منطق گزاره‌ای

۲-۳ منطق محمولات

۳-۳ منطق ساختی

تمرین‌ها

مراجع

۴- منطق شناختی (مدل‌سازی آگاهی)

۱-۴ منطق شناختی

۲-۴ دانش گروهی

۳-۴ منطق اعلان عمومی

۴-۴ عمل شناختی

۴-... منطق باور

۴ - ... منطق اعلان عمومی باور

۴-۵ مدل سازی

تمرین ها

مراجع

۵- منطق بازی (مدل سازی تعامل، ائتلاف، تکامل)

آشنایی کوتاه با نظریه بازیها

۵-۱ بازی های استاتیک

۵-۲ بازی های دینامیک

۵-۳ بازی های تکرارشونده

۵-۴ بازی های ائتلافی

۵ - ... بازی ها و سیستم های تکاملی

۵-... بازی های بیزی و طراحی مکانیسم

۵-۵ منطقی برای ترجیحات

۵-۶ منطقی برای ائتلاف

۵-۷ مدل سازی

تمرین ها

مراجع

۶- منطق تکلیف (مدل سازی تعهد)

۶-۱ منطق تکلیف

۶-۲ تنازع ها

۳-۶ سیستم‌های هنجاری^۳

۴-۶ بازی‌های هنجاری

۵-۶ مدل‌سازی

تمرین

مراجع

۷- منطق زمانی (مدل‌سازی همزمانی)

۱-۷ سیستم‌های انتقالی

۲-۷ منطق LTL

۳-۷ منطق CTL

۴-۷ مدل‌سازی

تمرین‌ها

مراجع

۸=.... شبکه‌های پتری^۴ (مدل‌سازی خودتنظیمی)

.....

.....

بخش سوم: ابزارهای پیاده‌سازی

۹- برنامه‌نویسی منطقی

Prolog ۱-۹

۱۰- برنامه‌نویسی عامل‌گرا^۵

BDI ۱-۱۰

3APL ۲-۱۰

مراجع

۱۱- آشنایی با بررسی‌گرهای مدل^۶

۱-۱۱ بررسی‌گرهای مدل منطق شناختی

۲-۱۱ بررسی‌گرهای مدل منطق بازی

۳-۱۱ بررسی‌گرهای مدل منطق تکلیف

۴-۱۱ بررسی‌گرهای مدل منطق زمانی

مراجع

مقدمه

چرا نظریه سیستم‌ها؟

۱. ریاضیات برای سیستم‌های اجتماعی: آنچه نیوتن را به یک دانشمند بزرگ تبدیل کرد، پی بردن او به افتدن سیب از درخت به زمین نبود، این را هر آدمی می‌دانست، بلکه **صورتبندی** تعدادی متناهی قوانینی ساده بود که به کمک آن قوانین ساده می‌توان اتفاقات پیچیده حرکت اشیا را تحلیل کرد. شاید قبل از نیوتن هیچ کس نمی‌توانست باور کند روزی به کمک تعدادی متناهی قوانین ساده و حساب دیفرانسیل بتوان به ماه سفر کرد. امروز نیز کسی نمی‌تواند باور کند که بتوان تعدادی متناهی قوانین ساده **صورتبندی** کرد که به کمک آنها اتفاقات پیچیده اجتماعی، سیاسی، حقوقی، اقتصادی و ... را تحلیل کنیم. درس نظریه سیستم‌ها به آغاز و روزنه‌ای کوچک برای پیدا کردن این تعداد متناهی **قوانین ساده** می‌اندیشد که به همراه منطق و روش‌های صوری و ابزارهای کامپیوتری بتوان سیستم‌های پیچیده اجتماعی را تحلیل کرد.

۲. چرچیل یا انیشتین؟ در هر نسل از جامعه همواره تعدادی افراد با تواناییهای قابل ملاحظه وجود دارند که سیستم اجتماعی باید از هدر رفتن توانایی آنها جلوگیری کند. سیستم باید بتواند نخبگان را به نسبت‌های مورد نیاز بین **علوم انسانی**، علوم پایه، فنی، و پزشکی توزیع کند. اگر این توزیع به طور مناسب صورت نگیرد آنگاه جامعه با بحرانی عظیم برای مدت زمانی طولانی روبرو خواهد بود. متأسفانه به نظر نمی‌رسد در ایران سیاستی برای این امر وجود داشته باشد که ما در آینده چه تعدادی از نخبگانمان باید سیاستمدار، چه تعداد جامعه‌شناس، روانشناس، ریاضیدان، فیزیکدان، اقتصاددان، حقوقدان، مهندس، و پزشک بشوند. با مد شدن پزشکی و مهندسی اکثر نخبگان نسل کنونی به اشتباه تنها در این دو گرایش علمی جمع شده‌اند، و با یک بی‌فرهنگی بزرگ رشته‌های علوم-انسانی **بی‌ارزش** جلوه داده شده‌اند. علوم انسانی بر خلاف آنچه در دبیرستان‌ها تبلیغ می‌شود یک علم حفظی نیست، بلکه یک علم تحلیلی هزاران بار پیچیده‌تر از علوم پایه و فنی است، که هنوز برای صورتبندی قوانین آن و بکار بستن ریاضیات در آن باید تلاش کرد. **جامعه ایرانی به امیر کبیر^۷ بیش‌تر (و پیش‌تر) از انیشتین نیاز دارد.**

۳. دانشجوی: دانشجو باید پس از پایان درس به سه بخش اصلی ارائه شده تسلط پیدا کند. ۱. با سیستم‌های اجتماعی آشنا باشد و این پرسش را در ذهن خود داشته باشد که چگونه می‌تواند نیوتن سیستم‌های اجتماعی شود و ریاضیاتی برای سیستم‌های اجتماعی صورتبندی کند. ۲. بتواند یک سیستم اجتماعی را به درستی به کمک منطق مدل‌سازی کند. ۳. بتواند با ابزارها مربوط مدل‌سازی خود را پیاده‌سازی کند. ۴. امید می‌رود درکی تحلیلی از اتفاقات سیاسی-اجتماعی که هر روز در اطراف ما اتفاق می‌افتد داشته باشد. ۵. کار گروهی و تقسیم کردن کار در یک گروه را تمرین کند.^۸

۴. اقلیدس ریاضیات (خواص و روابط) **اشیا ساکن** را صورتبندی کرد، نیوتن ریاضیات **اشیا متحرک**، و حالا بشر می‌خواهد ریاضیات **اشیا هوشمند** را صورتبندی کند.

^۷ روانش شاد.

^۸ این توانایی‌ها از دانشجویان درس انتظار می‌رود که از مدرس درس بسیار باهوش‌تر و کوشاتر هستند.

سیستم اجتماعی

یک دیدگاه در مطالعه علوم اجتماعی (علوم سیاسی، اقتصاد، حقوق و . . .) روش پایین به بالا است. به این ترتیب که ویژگی‌های جمعی را به ویژگی‌های فردی کاهش می‌دهند. سیستم‌های اجتماعی از تعدادی عامل تشکیل می‌شوند که با هم تبادل اطلاعات می‌کنند، بر سر منابع موجود رقابت و ائتلاف می‌کنند، و به یکدیگر برای انجام کارهایی متعهد می‌شوند. به این ترتیب ویژگی‌های زیر را برای یک عامل اجتماعی در نظر می‌گیریم.

۱. آگاهی

۲. تعامل (رقابت)

۳. ائتلاف

۴. تعهد

۵. همزمانی

هدف این درس آشنایی با سیستم‌های اجتماعی^۹ و مدل‌سازی منطقی آنها است.

منظور ما از سیستم اجتماعی (چند عاملی) هر سیستمی است که چند عامل در کنار یکدیگر با هم کار می‌کنند. برای مثال، بازی‌های اقتصادی، پروتکل‌های امنیت، مذاکرات دیپلماتیک، پیروان یک مذهب، و . . . نمونه‌هایی از سیستم‌های اجتماعی (چندعاملی) هستند. توجه کنید که در یک سیستم اجتماعی عاملها مختار هستند و هر عامل به دنبال به تحقق رساندن اهداف خویش است. به یک جامعه که در آن یک نفر فرمانده و بقیه فرمانبر هستند سیستم اجتماعی نمی‌گوییم. برای مثال، انگشتان دست یک سیستم تک عاملی است نه یک سیستم اجتماعی (چندعاملی). برای آنکه کارامدی یک سیستم

^۹ واژه‌های روبرو را در اینترنت جستجو کنید Complex systems, Social systems, Multi-agent systems

اجتماعی بالا رود دو نکته باید در نظر گرفته شود: ۱- **عاملها به کار هم کار نداشته باشند** ۲- **عاملها با هم همکاری کنند.**

پروتکل (الگوریتم چندعاملی)

یک پروتکل یا یک الگوریتم چندعاملی عبارت است از مشخص کردن اینکه هر عامل باید چه عملی را انجام دهد تا هدف مورد نظر برای سیستم اجتماعی 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. برای مثال از پروتکل‌های اجتماعی ۲-۲-۶-۲ حراجی‌ها و ۲-۳-۲ بریدن کیک را ببینید. پس از طراحی پروتکل، باید با روش صوری و منطقی نشان داد که پس از اجرای پروتکل ویژگی‌های مورد نظر برآورده می‌شوند.

مدل‌سازی منطقی (شرح، توصیف، درستیابی)

مدل‌سازی منطقی یک سیستم از سه قسمت تشکیل می‌شود

۱. **شرح**^{۱۰} سیستم به وسیله یک مدل ریاضی (منطقی)

۲. **توصیف**^{۱۱} ویژگی‌های مورد نظر به کمک گزاره‌های منطقی

۳. **درستیابی**^{۱۲} ویژگی‌های توصیف شده در مدل ریاضی سیستم.

در این درس، برای مدل‌سازی منطقی سیستم‌های اجتماعی و توصیف ویژگی‌های، آگاهی، تعامل (رقابت)، ائتلاف، تعهد، و همزمانی از منطق‌های

۱. **منطق شناختی** Epistemic Logic (مراجع [۱، ۴، ۹] را ببینید)

۲. منطق بازی Game Logic (مراجع [۳،۴،۶] را ببینید)

۳. منطق تکلیف Deontic Logic (مراجع [۲،۹] را ببینید)

۴. منطق زمانی Temporal Logic (مراجع [۵،۴] را ببینید)

بهره می‌بریم. هر یک از منطق‌های فوق می‌تواند به عنوان یک درس ۴ واحدی کارشناسی ارشد (تحت عنوان منطق پیشرفته یا مباحثی در منطق) ارائه شود. هدف درس نظریه سیستم‌ها پوشاندن کامل این ۴ نوع منطق نیست، بلکه آشنایی و ایجاد علاقه به این منطق‌ها و چگونگی مدل‌سازی کردن سیستم‌های اجتماعی به کمک آنها است. دانشجوی در صورت علاقه به هر کدام از ۴ مورد فوق، برای تکمیل دانش خود باید به مراجع ذکر شده رجوع کند. درس نظریه سیستم‌ها از کنار هم گذاشتن این ۴ منطق با هدف ایجاد یک ایده برای مدل‌سازی سیستم‌های اجتماعی تشکیل می‌شود.

مراجع

1. H. van Ditmarsch, W. van der Hoek, B. Kooi. **Dynamic Epistemic Logic**, Springer, 2008.
2. J. F. Horty. **Agency and Deontic Logic**, Oxford University Press, 2001.
3. M. Pauly, **Logic for Social Software**, PhD Thesis, ILLC, 2001.
4. S. van Otterloo, **A Strategic Analysis of Multi-agent Protocols**, PhD Thesis, ILLC, 2005.
5. C. Bair, J. P. Katoen, **Principles of Model Checking**, MIT Press, 2008.
6. J. N. Webb, **Game Theory, decision, interaction, and evolution**, Springer, 2007.
7. Yoram Bauman, **Quantum Microeconomics**, 2005.

بخش اول علوم اجتماعي

آشنایی کوتاه با نظریه‌های علوم اجتماعی

.....

سیستم‌های اجتماعی (چندعاملی)

منظور ما از یک سیستم اجتماعی (چندعاملی) هر سیستمی است که چند عامل مختار در کنار یکدیگر در آن کار می‌کند تا منافع خود را برآورده سازند. در این فصل، نمونه‌هایی از سیستم‌های اجتماعی را با توجه به ویژگی‌های آگاهی، تعامل، ائتلاف، تعهد، همزمانی، تکامل، خودتنظیمی و نیازها عاملها معرفی می‌کنیم.



یک دسته از پرندگان که در حال مهاجرت از دریای کاسپین^{۱۳} به خلیج فارس هستند را می‌توان به عنوان نمونه‌ای از سیستم‌های اجتماعی در نظر گرفت. پرندگان بصورت بسیار منظم در کنار هم پرواز می‌کنند. آنها نه پراکنده می‌شوند و نه با هم برخورد می‌کنند. این نظم چگونه شکل می‌گیرد؟ دو پاسخ متفاوت زیر را می‌توان در ممکن دانست:

¹³ قزوین

۱. راهبری تک عاملی: پرنده‌ای به عنوان راهبر گروه وجود دارد که پرندگان دیگر با توجه به او مسیر حرکت خود را مشخص می‌کنند. اگر پرنده به راست منحرف شود، همه به راست منحرف می‌شوند، و اگر به چپ منحرف شود آنگاه همه به چپ منحرف می‌شوند. به این ترتیب نظم حاصل پیروی از یک عامل راهبر می‌باشد.

۲. راهبری چند عاملی: الف. هر پرنده‌ای بویی از خود متصاعد می‌کند که در فضا پخش می‌شود ب. هر پرنده سعی می‌کند که در موقعیتی حرکت کند که مقدار معینی از بو را استشمام می‌کند. در این حالت هر پرنده‌ای به نوعی نقشی در راهبری گروه بازی می‌کند.

در این جزوه به بررسی سیستم‌های اجتماعی با توجه به پاسخ دوم خواهیم پرداخت. هر عامل در یک سیستم اجتماعی یک عامل منطقی^{۱۴} است که آگاهی‌ها و باورهای معینی دارد که در ارتباطات تغییر می‌کنند. برای برآورده کردن نیازها و منافع خود با عامل‌های دیگر ائتلاف و رقابت می‌کند. تعهداتی اجتماعی نسبت به عامل‌های دیگر دارد که در صورت تخطی از آنها توسط اجتماع مجازات می‌شود. در بخش ۲ جزوه برآنیم تا این مفاهیم را به کمک منطق‌های شناختی، بازی، و تکلیف مدل کنیم.

۱-۲ آگاهی

آگاهی هر عامل در یک سیستم با توجه به میزان دسترسی عامل به اطلاعات سیستم مشخص می‌شود. مثلا یک مدیر می‌تواند دسترسی بیشتری به اطلاعات نسبت به معاونین خود داشته باشد. آگاهی هر عامل نقش اساسی در چگونه عمل کردن او در سیستم چندعاملی دارد. در زیر نمونه‌هایی از سیستم-های اجتماعی (چندعاملی) را با توجه به آگاهی عامل‌ها معرفی می‌کنیم. مفهوم آگاهی در فصل ۲ توسط منطق شناختی مدل می‌شود.

۱-۱-۲ حاصلجمع و حاصلضرب

از دو عدد $1 < x < y$ که $x + y \leq 100$ ، جمع دو عدد به سارا و حاصلضرب دو عدد به پارسا گفته شده است. سارا و پارسا گفتگو زیر را انجام می‌دهند.

پارسا: من نمی‌دانم که این دو عدد چیست؟

سارا: من هم نمی‌دانم.

پارسا: حالا من می‌دانم که دو عدد چیست.

سارا: اکنون من هم دو عدد را می‌دانم.

دو عدد x, y چه اعدادی هستند؟

۲-۱-۲ کودکان گلی

سه کودک با نامهای a ، b و c بعد از بازی در کنار یک ساحل به خانه برمی‌گردند.

(۱) برای هر کودک این امکان وجود دارد که پیشانی او در هنگام بازی گلی شده باشد.

۲) هر کودک فقط پیشانی دو کودک دیگر را می بیند و نمی تواند پیشانی خود را ببیند.

فرض کنید که دو کودک از سه کودک گلی باشند. پدر سه کودک خطاب به آنها می گوید

پیشانی حداقل یکی از شما گلی است. آنها که می دانند که پیشانی آنها گلی است یک گام جلو بیایند.

اما هیچ کودکی جلو نمی آید. پدر دوباره گزاره بالا را می گوید. سپس دو کودک گلی همزمان از صف

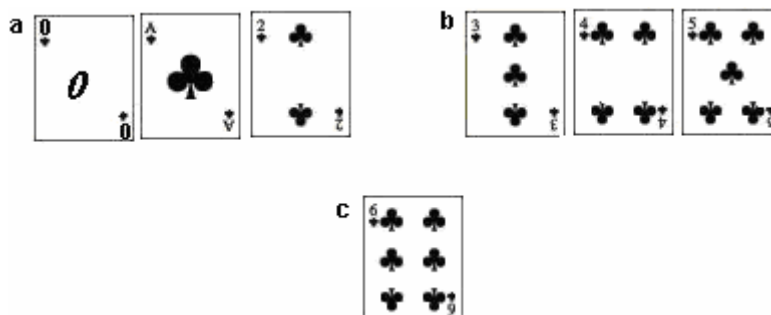
خارج می شوند. چگونه این اتفاق می افتد؟

۲-۱-۳ بازی کارتهای روسی

یک دسته ۷ تایی کارت که روی آنها اعداد 0,1,2,3,4,5,6 نوشته شده است بین سه عامل a ، b و c

توزیع شده است، به طوریکه به دو عامل a و b هر نفر سه کارت، و به عامل c یک کارت داده شده

است.



عاملهای a و b می خواهند همدیگر را از کارتهای خود مطلع کند بدون آنکه عامل c اطلاعی در

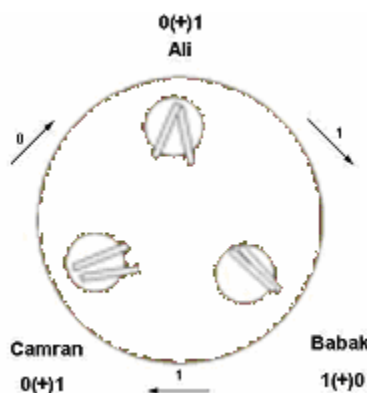
مورد دست آنها پیدا کند. اما سیستم ارتباطی به گونه ای است که هر خبری را که یکی از عاملها برای

عاملی دیگر می فرستد، همه عاملها از آن مطلع می شوند. یعنی ارتباط دو عامل تنها از راه اعلان عمومی

میسر است. در بخش ۲ به کمک منطق شناختی، به درستیابی پروتکل های ارتباطی اعلان عمومی برای

تبادل اطلاعات دو عامل a و b ، به طوریکه عامل c هیچ اطلاعی در مورد توزیع کارتها پیدا نکند، خواهیم پرداخت.

۴-۱-۲ شام خوردن سه رمزنگار



سه رمزنگار a, b, c دور یک میزگرد شام می‌خورند. بعد از شام متوجه می‌شوند که صورت حساب پرداخته شده است. در مورد این موضوع که یا یکی از رمزنگارها صورت حساب را پرداخته است یا سازمان امنیت کشور توافق (همه‌دانی مشترک) وجود دارد.

رمزنگارها می‌خواهند بدانند که آیا یکی از آنها پرداخت کننده بوده است یا سازمان امنیت. اما آنها می‌خواهند در صورتی که یکی از آنها پرداخت کننده باشد هویت او لو نرود و گمنام باقی بماند.

به این منظور پروتکل زیر را اجرا می‌کنند:

هر رمزنگار یک رقم 0 یا 1 را به دلخواه برای خود انتخاب می‌کند. سپس به طور خصوصی رقم خود را به نفر سمت چپ خود اعلان می‌کند. هر رمزنگار رقم دریافتی را (رقمی را که از نفر سمت راستی خود دریافت کرده است) با رقم انتخابی خود (رقمی که انتخاب کرده و به نفر سمت چپی خود فرستاده است) فصل ضمنی (XOR) می‌کند. اگر پرداخت کننده نباشد حاصل را به طور عمومی اعلان می‌کند

وگرنه حاصل را با 1 جمع دودویی می‌کند و حاصل جمع جدید را به طور عمومی اعلان می‌کند. سه رقمی که اعلان عمومی شده است با هم جمع دودویی می‌شوند. اگر حاصل 0 باشد یعنی سازمان امنیت پرداخت کننده است، و اگر 1 باشد یعنی یکی از عاملها پرداخت کننده است.

چگونه مطمئن شویم که پروتکل فوق گمنامی را حفظ می‌کند؟

۵-۱-۲ اعدام شگفت آور

متهمی در دادگاه محکوم به مرگ می‌شود. قاضی دادگاه رو به متهم می‌کند و حکم زیر را قرائت می‌کند:

در صبح زود یکی از روزهای هفته آینده تو اعدام خواهی شد. اما اعدام به گونه‌ای خواهد بود که تو نمی‌توانی آن روز را پیش‌بینی کنی و به این ترتیب آن روز موقعی که از خواب برای اعدام بیدار می‌شوی شگفت زده خواهی شد.

متهم بعد از شنیدن حکم، با غمگینی به سلولش منتقل می‌شود. بعد از مدتی با خوشحالی رو به هم سلولی خود می‌کند و می‌گوید قاضی نمی‌خواهد مرا اعدام کند! و استدلال زیر را بیان می‌کند.

قاضی در صبح جمعه هفته آینده مرا اعدام نمی‌کند. زیرا در شب پنج‌شنبه من می‌توانم اعدام فردا را پیش‌بینی کنم و حکم قاضی نقض می‌شود. قاضی نمی‌تواند مرا صبح پنج‌شنبه نیز اعدام کند. چون من شب چهارشنبه می‌دانم که از دو صبح باقیمانده، او مرا در صبح جمعه اعدام نمی‌کند و فقط صبح پنج‌شنبه باقی می‌ماند. که دوباره چون من شب چهارشنبه می‌توانم صبح اعدام خود را پیش‌بینی کنم، حکم قاضی نقض می‌شود. با همین استدلال روزهای دیگر هفته نیز امکان اعدام من وجود ندارد.

اما متأسفانه در صبح چهارشنبه هفته آینده متهم اعدام می‌شود!!!

(به کمک منطق شناختی، این پارادوکس را مدل خواهیم کرد).

۶-۱-۲ کارآگاه علوی (دانش توزیع شده)

کارآگاه علوی به دنبال بررسی یک قتل برای پیدا کردن قاتل مینا حقایق زیر را برای قاضی آشکار می-کند

۱. در هنگام قتل، چاقوی آشپزخانه در کمد اتاق خواب قرار داشته است.

۲. اگر لیلا بداند که در هنگام قتل چاقوی آشپزخانه در کمد اتاق خواب قرار داشته است آنگاه

همسر لیلا بی گناه است.

اتفاقاً لیلا می‌داند که در هنگام قتل چاقوی آشپزخانه در کمد اتاق خواب قرار داشته است. کارآگاه

علوی به سمت لیلا راه می‌افتد تا از لیلا که در حیاط دادگاه ایستاده است در مورد مکان چاقوی

آشپزخانه سوال بپرسد. اما قبل از اینکه کارآگاه علوی به لیلا برسد، یک خبرنگار فضول در بلندگوی

دادگاه اعلان عمومی می‌کند که

در هنگام قتل چاقوی آشپزخانه در کمد اتاق خواب قرار داشته است.

بعد از این اعلان، کارآگاه علوی دیگر نمی‌تواند بی‌گناهی همسر لیلا را اثبات کند!!! چرا؟

۷-۱-۲ سردارهای متحد (همه‌دانی مشترک)

دو فرمانده متحد a, b همراه با لشگرهایشان روی دو قله کوه، که در دره بین دو قله لشگر دشمن قرار

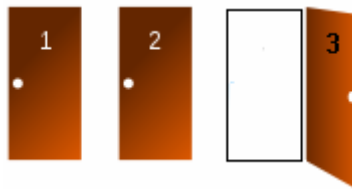
دارد، کمین کرده‌اند. اگر هر دو سردار همزمان به دشمن حمله کنند پیروز می‌شوند و اگر در زمانهای

متفاوت حمله کنند شکست خواهند خورد. فرمانده a پیکی را با پیام زیر برای فرمانده b می‌فرستد.

فردا صبح هنگام طلوع به دشمن حمله کنیم φ

پیک مجبور است دره بین دو قله را رد کند و همیشه احتمال اینکه به دست دشمن اسیر شود هست. فرض کنید پیک بتواند به سلامت دره را رد کند و خبر را به فرمانده دیگر برساند. فرمانده a گزاره φ را می‌داند و فرمانده b نیز می‌داند که فرمانده a گزاره φ را می‌داند. آیا فرمانده‌ها حمله می‌کنند؟ خیر، توافقی بین فرمانده‌ها اتفاق نیفتاده است. فرمانده a این حالت را ممکن می‌داند که پیک نتوانسته باشد به سلامت دره را رد کند. فرمانده a نمی‌داند که فرمانده b گزاره φ را می‌داند. حال فرض کنید فرمانده b از پیک می‌خواهد برگردد و خبر رسیدن پیام را به فرمانده خود بدهد. فرض کنید باز هم پیک به سلامت دره را رد کند. آیا فرمانده‌ها حمله می‌کنند؟

۸-۱-۲ مساله بازی تلویزیونی^{۱۵}



در یک بازی تلویزیونی، مجری به شرکت کننده می‌گوید: که شما سه درب با شماره‌های ۱، ۲ و ۳ در مقابل دارید. پشت یکی از این درب‌ها یک اتوموبیل سمند است و دو درب دیگر پوچ هستند. یکی از درب‌ها را انتخاب کنید. اگر پشت دربی که انتخاب کردید خودرو بود شما برنده خودرو خواهید بود. شرکت کننده یکی از درب‌های را (مثلاً ۲) انتخاب می‌کند. بعد از انتخاب شرکت کننده مجری یکی از دو درب دیگر (مثلاً ۳) را پوچ می‌کند و از شرکت کننده می‌پرسد که آیا حاضر است دری را که انتخاب کرده است (یعنی درب ۲) با دری که هنوز باز نشده است (درب ۱) عوض کند.

با منطق شناختی احتمالی می‌توان نشان داد که اگر شرکت کننده درب را عوض کند احتمال موفقیتش بیشتر می‌شود (مرجع [؟] را ببینید).

۹-۱-۲ باور مشترک نادرست

در انتخابات ریاست جمهوری کشور "نانا" دو فرد A, B از یک حزب سیاسی مشترک کاندید شده‌اند.

۱. همه هواداران این حزب سیاسی کاندید A را به کاندید B ترجیح می‌دهد.

۲. هواداران می‌دانند که اگر همه بطور متحد به یک کاندید رای ندهند کاندید حزب مخالف

رییس جمهور خواهد شد.

۳. همه این هواداران باور مشترک نادرستی دارند که دیگر هواداران حزب کاندید B را به A

ترجیح می‌دهند.

به این ترتیب، آنها همه به کاندید B رای می‌دهند!!!

۲-۲ تعامل (رقابت)

(توضیح در مورد رقابت- تعادل نش، پارتو، نظریه بازی‌ها)

۱-۲-۲ اسب کندروتر

دو مرد در حالی که در جنگل گلستان اسب سواری می‌کنند سر اینکه اسب کدام یک سریعتر است با یکدیگر بگومگو می‌کنند که در راه دختر ترکمنی جوان و زیبا را می‌بینند. هر یک از اسب سوارها دختر را دعوت می‌کنند که سوار اسبشان شود. ولی دختر از آنها می‌خواهد که تا سر یک تپه با هم مسابقه بدهند و او سوار اسبی می‌شود که کندتر حرکت کند زیرا او از اسب سواری می‌ترسد. اسب سوارها شروع به مسابقه می‌کنند اما بعد از مدتی می‌فهمند که این مسابقه پایان ندارد، چون هر اسب سوار علاقه دارد که با سرعت کمتر و کمتری حرکت کند. چه باید کرد؟

خاتونی پیر دو اسب سوار را می‌بیند که بازیچه دختری جوان شده اند. به آنها می‌گوید کافیهست که اسب‌های خود را با همدیگر عوض کنند و سپس تا سر تپه مسابقه بدهند!

این مساله را می‌توان برای دو بنگاه اقتصادی نیز در نظر گرفت. فرض کنید که دولت بخواهد تنها به یکی از دو بنگاه اقتصادی کمک کند، و قصد دولت این باشد که سود دهی دو بنگاه را در شش ماه بررسی کند و به بنگاهی که کمتر سود دهی دارد کمک مالی کند. این خواست دولت سبب تضرع و ضرر دهی هر دو بنگاه می‌شود.

۲-۲-۲ تنازع زندانی‌ها^{۱۶}

دو متهم هم دست توسط پلیس برای یک جنایت در سلول‌های جداگانه بازجویی می‌شوند. اگر هیچکدام به جنایت اعتراف نکنند قاضی با توجه به شواهد موجود هر یک را به ۲ سال حبس محکوم می‌کند. اگر هر دو به جنایت اعتراف کنند هر یک به ۴ سال حبس محکوم می‌شود. اگر یکی اعتراف کند و دیگری اعتراف نکند، فردی که اعتراف کرده است آزاد می‌شود و دیگری به ۵ سال حبس محکوم می‌شود. فکر می‌کنید که کدام حالت اتفاق می‌افتد؟

۳-۲-۲ سرمایه‌گذاری خصوصی - عمومی

۱۰۰ عامل در یک شهر کوچک زندگی می‌کنند که هر یک ۵ هزار تومان پول دارند. یک بانک در شهر است که دو نوع سرمایه‌گذاری را ارائه می‌دهد. ۱- سرمایه‌گذاری خصوصی ۲- سرمایه‌گذاری عمومی (۱) اگر یک عامل ۵ هزار تومان خود را سرمایه‌گذاری خصوصی کند در پایان سال ۱۰ هزار تومان سود می‌گیرد.

(۲) اگر یک عامل ۵ هزار تومان خود را سرمایه‌گذاری عمومی کند در پایان سال به همه عامل‌های شهر نفری ۵ هزار تومان سود می‌رسد.

برای مثال اگر هر ۱۰۰ نفر سرمایه‌گذاری عمومی کنند در پایان سال هر فرد ۵۰۵ هزار تومان پول دارد، و اگر هر ۱۰۰ نفر سرمایه‌گذاری خصوصی کنند در پایان سال هر نفر ۱۵ هزار تومان پول دارد. به نظر شما چند نفر سرمایه‌گذاری عمومی و چند نفر سرمایه‌گذاری خصوصی خواهند کرد؟

۴-۲-۲ بازی جوجه^{۱۷}

شیرین از دو خواستگارش فرهاد و خسرو می‌خواهد که مسابقه شجاعت بدهند و هر کس که شجاع تر باشد شیرین به او قول ازدواج می‌دهد. مسابقه به این صورت است که هر دو خواستگار باید سوار اتومبیل‌های پر سرعت خود شوند و به سمت یک صخره سنگی برانند. هر کس که اتومبیل خود را از مسیر مسابقه منحرف کرد جوجه است و دیگری شجاع است. اگر اتومبیل‌ها به صخره برخورد کنند هر دو خواستگار می‌میرند و شیرین هم منتظر دو خواستگار بعدی می‌ماند!^{۱۸}

۵-۲-۲ آربیتراژ ترافیک^{۱۹}

در یک ترافیک، انتظار می‌رود که همه خطوط حرکت سرعت تقریباً یکسانی داشته باشند. دلیل این است که آربیتراژ ترافیک خودش را از بین می‌برد. اگر یکی از خطوط با سرعت بیشتری حرکت کند، بعضی از رانندگان خط حرکت خود را به خط سریعتر عوض می‌کنند. اما موفقیت آنها طولی نخواهد کشید. خط سریعتر نیز پرتر و خط کندتر خالی تر می‌شود. به این ترتیب در نهایت همه خطوط سرعت یکسانی خواهند داشت. لازم به ذکر است که وجود رانندگانی که خط خود را عوض می‌کنند به آندسته از رانندگانی که در خط خود باقی می‌مانند کمک می‌کند. رانندگانی که خط خود را عوض نمی‌کنند بدون هیچ ریسک و تلاشی با سرعت بیشتری در همان خط حرکت خود که خالی تر می‌شود حرکت می‌کنند!!! به این ترتیب عدم رقابت کردن به ضرر همه است. آیا آربیتراژهای دیگری را می‌توانید نام ببرید که آربیتراژ خودش را از بین ببرد.

¹⁷ Chicken Game

¹⁸ جهان پیر است و بی‌بنیاد از این فرهاد کش فریاد (حافظ)

¹⁹ Rush-Hour Arbitrage

۶-۲-۲ انواع حراجی ها

فرض کنید می‌خواهید لپ تاپ خود را به حراج بگذارید. به کدامیک از روش‌های زیر این کار را می‌کنید؟

۱. فروش به بالاترین قیمت/اعلان شده

در این روش از متقاضیان خواسته می‌شود که قیمت مورد نظر خود را روی یک کاغذ نوشته، آن را در پاکت قرار داده و مخفیانه به فروشنده بدهند. سپس فروشنده در حضور همه متقاضیان، پاکت‌ها را باز کرده و لپ تاپ به متقاضی A که بیشترین قیمت را نوشته است، به همان قیمت فروخته می‌شود. مثلاً اگر A قیمت ۱۵۰ هزار تومان را نوشته باشد لپ تاپ به ۱۵۰ هزار تومان فروخته می‌شود.

۲. فروش به دومین قیمت بالا/اعلان شده

در این روش از متقاضیان خواسته می‌شود که قیمت مورد نظر خود را روی یک کاغذ نوشته، آن را در پاکت قرار داده و مخفیانه به فروشنده بدهند. سپس فروشنده در حضور همه متقاضیان، پاکت‌ها را باز کرده و لپ تاپ به متقاضی A که بیشترین قیمت را نوشته است به دومین قیمت بالا فروخته می‌شود. مثلاً اگر A قیمت ۱۵۰ هزار تومان را نوشته باشد و بیشترین قیمت ارائه شده به غیر از او ۷۰۰ هزار تومان باشد، لپ تاپ به ۷۰۰ هزار تومان فروخته می‌شود.

۷-۲-۲ بازی هزارپا^{۲۰}

۱۰ اسکناس ۵ هزار تومانی روی یک میز قرار دارد. دو بازیکن ۱ و ۲ به نوبت حرکت زیر را انجام می‌دهند. هر بازیکن در نوبت خود یا می‌تواند ۲ اسکناس را بردارد که در اینصورت بازی تمام می‌شود، یا

می‌تواند یک اسکناس را بر دارد که در اینصورت نوبت بازیکن بعدی می‌شود. هر بازیکن می‌خواهد بیشترین پول ممکن را بدست آورد. این بازی را به کمک منطق بازی تحلیل خواهیم کرد.

۸-۲-۲ تقسیم بستنی

دو کودک به صورت زیر یک بستنی را بین خود تقسیم می‌کنند. در هر مرحله یکی از دو کودک یک پیشنهاد برای تقسیم کردن بستنی می‌دهد. اگر کودک دیگر پیشنهاد را پذیرفت بستنی مطابق با پیشنهاد تقسیم می‌شود وگرنه نوبت کودک دیگر می‌شود که در مرحله بعد یک پیشنهاد تقسیم ارائه دهد. اما از هر مرحله به مرحله بعد نصف بستنی آب می‌شود. بازی وقتی تمام می‌شود که یکی از پیشنهادها پذیرفته شود. فرض کنید کودکان مجبور باشند حداکثر بازی را تا ۳ مرحله انجام دهند. کودکی که اول تقسیم کننده است چه پیشنهادی می‌دهد؟

۲-۳ ائتلاف

(توضیح در مورد بازیهای تعاونی و ...)

۲-۳-۱ بریدن کیک (تقسیم عادلانه)

فرض کنیم می خواهیم که یک کیک عادلانه بین n نفر تقسیم شود. الگوریتم زیر نمونه ای از الگوریتم های چند عاملی برای $n=3$ هستند.

تعریف: گوییم یک تقسیم کیک بین n عامل عادلانه است هرگاه هر عامل باور داشته باشد که حداقل $\frac{1}{n}$ کیک به او

رسیده است

الگوریتم چند عاملی زیر عادلانه بودن تقسیم را برآورده می کند.

۱- ابتدا بازیکن ۱ کیک را به دو قسمت مساوی از لحاظ خود تقسیم می کند (فرض کنید

(a_1, a_2)

۲- بازیکن ۲ یکی از دو قسمت را که (از لحاظ خود) از دیگری بزرگتر است برای خود بر می -

دارد (فرض کنید a_2 را برداشته است)

۳- بازیکن ۱ قسمت خود را به ۳ قسمت مساوی (از لحاظ خود) تقسیم می کند (فرض کنید

(a_{11}, a_{12}, a_{13})

۴- بازیکن ۲ قسمت خود را به ۳ قسمت مساوی (از لحاظ خود) تقسیم می‌کند (فرض کنید

$$(a_{21}, a_{22}, a_{23})$$

۵- بازیکن ۳ از ۳ قسمت a_{11}, a_{12}, a_{13} بزرگترین قسمت (از لحاظ خود) را برمی‌دارد.

(فرض کنید a_{12})

۶- بازیکن ۳ از ۳ قسمت a_{21}, a_{22}, a_{23} بزرگترین قسمت (از لحاظ خود) را برمی‌دارد.

(فرض کنید a_{21})

بعد از انجام الگوریتم بازیکن ۱ قسمت‌های a_{11}, a_{13} ، بازیکن ۲ قسمت‌های a_{22}, a_{23} و بازیکن ۳

قسمت‌های a_{12}, a_{21} را خواهد داشت. به کمک منطق بازیها الگوریتم فوق را توصیف و درستیابی

می‌کنیم و نشان می‌دهیم که اگر دو عامل با هم ائتلاف کنند باز هم الگوریتم تضمین می‌کند که به

عامل دیگر حداقل $\frac{1}{3}$ یک (از لحاظ خود عامل) رسیده است.

۲-۳-۲ بریدن کیک (تقسیم حسادت-آزاد)

تعریف: گوییم یک تقسیم کیک بین n عامل از حسادت آزاد است هرگاه هیچ عاملی به عاملی دیگر حسادت نکند

الگوریتم چند عاملی زیر به یک تقسیم حسادت آزاد منجر می‌شود.

۱. بازیکن اول کیک را به سه قسمت a_1, a_2, a_3 از لحاظ خود مساوی تقسیم می‌کند.

۲. بازیکن دوم سه قسمت تقسیم شده را از لحاظ خود از بزرگ به کوچک مرتب می‌کند. فرض کنید $a_1 \geq_2 a_2 \geq_2 a_3$. سپس تکه $e \geq 0$ را طوری از a_1 جدا می‌کند که $a_1' = a_1 - e =_2 a_2$ شود.

۳. بازیکن سوم از بین تکه‌های a_1', a_2, a_3 تکه بزرگتر از لحاظ را انتخاب می‌کند و برای خود بر می‌دارد.

۴. اگر بازیکن سوم a_1' را بر ندارد a_1' به بازیکن دوم داده می‌شود و تکه دیگر باقیمانده (از سه تکه a_1', a_2, a_3) به بازیکن اول داده می‌شود. اگر بازیکن سوم a_1' را بردارد، بازیکن دوم از بین دو قسمت a_2, a_3 بزرگترین را از لحاظ خود انتخاب می‌کند و برای خود بر می‌دارد. تکه دیگر باقیمانده نیز به بازیکن اول داده می‌شود.

۵. بعد از اجرای ۴، یا بازیکن دوم یا بازیکن سوم a_1' را دارد. آن بازیکنی که a_1' را دارد بازیکن $P1$ و بازیکن دیگر (از بین بازیکن‌های دوم و سوم) را بازیکن $P2$ بنامید.

۶. بازیکن $P2$ قسمت e را به سه قسمت از لحاظ خود مساوی تقسیم می‌کند و بازیکن $P1$ ، بازیکن اول و بازیکن $P2$ به ترتیب هر یک، یک قسمت را برای خود بر می‌دارد.

آیا دو عامل می‌توانند بگونه‌ای ائتلاف کنند که بعد از انجام الگوریتم چند عاملی فوق، عامل دیگر به یکی از آنها حسادت کند.

۲-۳-۳ داد و ستد

نگار و فریمه در جزیره ابوموسی هستند. برای غذا، تنها دو راه وجود دارد

۱. ماهی گیری،

۲. جمع کردن میوه.

هر دو آنها تنها ۶ ساعت از روز را به جستجوی غذا می پردازند. هر فردی دوست دارد که در آخر روز به

اندازه برابری ماهی و میوه بخورد.

نگار در ماهی گیری از فریمه بهتر است. نگار در یک ساعت ۲ ماهی می گیرد در حالیکه فریمه می تواند

در یک ساعت ۱ ماهی بگیرد. فریمه نیز در جمع کردن میوه از نگار بهتر است. فریمه در یک ساعت ۲

میوه جمع می کند در حالیکه نگار می تواند ۱ میوه جمع کند. اگر داد و ستد امکان پذیر نباشد (نگار و

فریمه در دو جزیره جدا از هم باشند) با توجه به اینکه که فریمه دوست دارد که در آخر روز تعداد

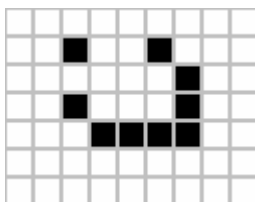
ماهی هایش با تعداد میوه هایش برابر باشد او حداکثر چند میوه و چند ماهی خواهد خورد؟ اگر داد و

ستد امکان پذیر باشد فریمه چند میوه و چند ماهی خواهد خورد؟

۲-۳-۴ مانع شدن از ورود به بازار

۲-۳-۵ منع و تله اجتماعی^{۲۱}

۲-۳-۶ بازی زندگی^{۲۲}



صفحه نامتناهی دو بعدی شطرنجی را در نظر بگیرید. هر خانه صفحه را یک سلول می‌نامیم که اگر خانه سیاه باشد می‌گوییم سلول زنده است وگرنه می‌گوییم سلول بی‌جان است. هر سلول با ۸ سلول همسایه خود تعامل می‌کند. در لحظات گسسته از زمان تغییرات زیر اتفاق می‌افتد.

۱. هر سلول زنده با کمتر از دو همسایه زنده از تنهایی می‌میرد.

۲. هر سلول زنده با بیشتر از ۳ همسایه زنده از کمبود اکسیژن می‌میرد.

۳. هر سلول زنده با دو همسایه زنده یا با ۳ همسایه زنده، به زندگی خود ادامه می‌دهد.

۴. هر سلول بی‌جان با دقیقاً ۳ همسایه زنده، زنده می‌شود.

بازی زندگی یک سیستم اجتماعی است که خود را تنظیم می‌کند. با یک نسل اول (یک مجموع از خانه‌های سیاه) بازی آغاز می‌شود، و نسل‌های بعدی در لحظات آینده به وجود می‌آیند.

۲-۳-۷ دزدان دریایی^{۲۳}

۵ دزد دریایی با نام‌های A, B, C, D, E ۵۰۰ سکه طلا پیدا می‌کنند. در بین این ۵ دزد دریایی سلسله مراتب قدرت بصورت $A > B > C > D > E$ وجود دارد و هر عامل رییس همه عامل‌هایی است که در مرتبه پایین‌تری از او قرار دارند. دزدان دریایی تصمیم می‌گیرند که بصورت زیر سکه‌ها را بین

خود تقسیم کنند. در هر مرحله عامل قویتر یک پیشنهاد برای تقسیم سکه‌ها می‌دهد و مشخص می‌کند که به هر عاملی چند سکه از ۵۰۰ سکه برسد. تقسیم به رای گذاشته می‌شود (عامل پیشنهاد دهنده نیز در صورتی که نتیجه رای گیری از بقیه عاملها برابر شد، می‌تواند رای بدهد) و اگر پیشنهاد پذیرفته شود که سکه‌ها تقسیم می‌شود وگرنه عامل قویتر را به داخل آب می‌اندازند تا کوسه‌ها او را بخورند و نوبت عامل قویتر بعدی می‌شود که پیشنهاد تقسیم ارایه دهد. فکر می‌کنید بازی به چه صورت انجام خواهد شد؟ دقت کنید که هر دزد می‌خواهد زنده بماند و بیشترین سهم را بدست آورد و از اینکه دزدی دیگر توسط کوسه‌ها خورده شود استقبال می‌کند. حالتی را در نظر بگیرید که به هر دزد یک عدد به عنوان قدرت او نسبت داده شود، و برای آنکه دزدان دیگر بتوانند آن دزد را به داخل آب بیندازند باید مجموع قدرت‌های آنها بیشتر باشد. در این حالت دزدها می‌توانند با هم ائتلاف کنند. مثلاً ممکن است A مجبور شود با E (ضعیف‌ترین دزد) ائتلاف کند. به تحلیل این بازی به کمک منطق بازی خواهیم پرداخت.

۲-۳-۸ کشورها و منابع مشترک.

چهار کشور با نام‌های USA, RUSSIA, IRAN, KUBA را با سه منبع A, B, C در نظر بگیرید.

○ کشورهای R, I بطور مشترک به منبع C دسترسی دارند،

○ کشورهای U, K بطور مشترک به منبع B دسترسی دارند، و

○ کشورهای U, R بطور مشترک به منبع A دسترسی دارند.

هر کشوری سعی می‌کند که بیشترین مقدار ممکن را از منابع برداشت کند. تابع

$p : \{U, R, I, K\} \times TIME \rightarrow \mathbb{Q}$ قدرت هر عامل را در هر سال نشان می‌دهد. در هر سال

می‌توان از منبع A a واحد، از منبع B مقدار b واحد، و از منبع C مقدار c واحد برداشت کرد. هر

عامل با توجه به قدرتش می‌تواند درصد استخراج خود را مشخص کند. مثلاً اگر R قدرتش دو برابر I

است از منبع C مقدار $\frac{2}{3}C$ را استخراج می‌کند. قدرت هر عامل در سال بعد برابر خواهد بود با قدرت سال قبل او به علاوه مقدار واحدی که استخراج کرده است. عاملها می‌توانند در شروع هر سال قدرت به هم غرض بدهند (با هم ائتلاف کنند). با توجه به مقدارهای a, b, c و قدرت عاملها، فکر می‌کنید که چه عاملهایی باید با هم متحد شوند.

۹-۳-۲ پروتکل انتخاباتی

در یک کشور مردم‌سالار، ۴۹٪ از گروه (الف) و ۵۱٪ از گروه (ب) هستند. در انتخابات، هر فرد تنها به کاندیدایی رای می‌دهد که از گروه خود او باشد. به این ترتیب، با توجه به اینکه گروه (ب) در اکثریت است، همواره رئیس‌جمهور از گروه (ب) خواهد بود. فعالان سیاسی گروه (الف) به این موضوع معترض هستند و گزاره زیر را معادل مردم‌سالاری می‌دانند که

اگر t درصد یک جامعه از یک گروه باشند، در یک جامعه مردم‌سالار در هر صد دوره t بار رئیس-

جمهور باید از اعضای این گروه باشد.

آیا می‌توانید پروتکلی انتخاباتی طراحی کنید که گزاره بالا را برآورده سازد.

۲-۴ تعهد

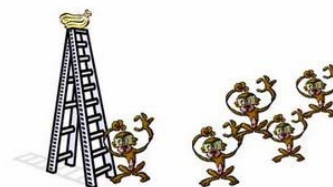
در یک اجتماع، عاملها می‌توانند نسبت به انجام بعضی کارها به همدیگر متعهد شوند و مجازات‌هایی را برای شکستن تعهد بین خود در نظر بگیرند. یک مساله‌ای که با آن روبرو می‌شویم آن است که چگونه استدلال کنیم که یک فرد به تعهد خود پایبند بوده است یا نه؟

۲-۴-۱ میمون‌ها و موز

گروهی از دانشمندان میمون را در قفسی قرار دادند. در وسط قفس یک نردبان و بالای نردبان موز گذاشتند.



پس از مدتی، هر وقت که میمونی بالای نردبان می‌رفت سایرین او را کتک می‌زدند.



پس از مدتی دیگر هیچ میمونی علی‌رغم وسوسه‌ای که داشت جرأت بالا رفتن از نردبان را به خود نمی‌داد.

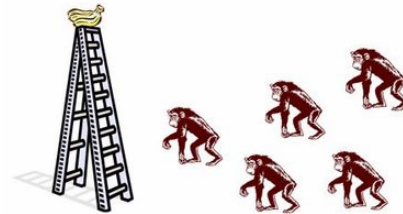


دانشمندان تصمیم گرفتند که یکی از میمون‌ها را جایگزین کنند. اولین کاری که این میمون جدید انجام داد این بود که بالای نردبان برود که بلافاصله توسط سایرین مورد ضرب و شتم قرار گرفت.

پس از هتدبیا کتک خوردن میمون جدید با این که نمی‌دانست چا اما یاد گرفت که بالای نردبان نرود.



میمون دومی جایگزین گردید و همان اتفاق تکرار شد. سومین میمون هم جایگزین شد و دوباره همان اتفاق (کتک خوردن) تکرار گردید. به همین ترتیب چهارمین و پنجمین میمون نیز عوض شدند.



آن چیزی که باقی مانده بود گروهی متشکل از ب میمون بوده که با این که هیچگاه آب سردی بر روی آن‌ها پاشیده نشده بود، میمون‌ها که بالای نردبان می‌رفت را کتک می‌زدند.



۲-۴-۲ بزهای هوشمند

۱۰ بز هوشمند در بیشه ای زندگی می کردند که تنها ۱۰ متر مربع آن برای چریدن قابل استفاده بود.

این بزهای هوشمند بر سر این ۱۰ متر مربع می جنگیدند و با شاخ های خود همدیگر را زخمی می

کردند. مدتی گذشت و بزها هوشمند به یک واقعیت پی بردند که :

- اگر جنگیدن را ادامه دهیم نسل ما که بزهایی هوشمند هستیم از بین می رود **اصل بقا**، یعنی حفظ نسل، مهمترین و مقدس ترین اصل زندگی ما بزهای هوشمند است. پس باید چاره ای بیندیشیم .

بزها چاره ای اندیشیدند و آن این بود که هر یک از ده بز یک متر مربع را **مالک** شود و همه با هم **تعهدی** مقدس کنند که به علف همدیگر تجاوز نکنند و به روزی حلال (علف حلال) خود قناعت کنند . به این ترتیب صلح و آرامش بیشه را گرفت و نسل بزها به سرعت (به علت نبود جنگ) افزایش یافت. بزها تولید مثل می کردند و هر بزی از پدر خود قسمتی از چراگاه را به ارث می برد. تا اینکه تعداد بزها به ۱۰۰۰ رسید و علفی که در ده سانتیمتر مربع یافت می شد برای زندگی یک بز کافی نبود و اگر هر بزی تنها به ده سانتیمتر قناعت می کرد همه بزها نابود می شدند و نسل بزهای هوشمند از بین می رفت. بزها اندیشیدند.

- از آنجا که مهمترین و مقدس ترین اصل این است که هیچگاه نسل بزهای هوشمند (همانند دایوناسورها) نباید از بین برود و قناعت کردن به روزی حلال و عمل به تعهد مقدس سبب نابودی همه ما بزها می شود پس دیگر نباید به روزی حلال قناعت کرد و شاخ زدن به یکدیگر عملی مقدس در جهت حفظ بقا اعلام می شود ²⁴.

۲-۴-۳ تنازع اخلاقی ^{۲۵} راننده

آقای A با سرعت قانونی در حال رانندگی است که متوجه می شود ترمز ماشین کار نمی کند. در مقابل او دو مسیر وجود دارد. یک مسیر بسته است و به دیواری بتنی ختم می شود که برخورد اتومبیل با دیوار

²⁴ فرق انسان با یک بز هوشمند چیست؟ هر دو این موجودات هوش دارند ولی اولی توانایی آبادانی کردن دارد. اگر انسان آبادانی نکند و منابع قابل دسترسی خود را افزایش ندهد، هوشمند بودن او نسلش را از بین می برد!؟

بتنی با سرعت قانونی به مرگ راننده منجر می‌شود. یک مسیر دیگر باز است اما دختری ۵ ساله در وسط مسیر دارد عروسکش را که از دستش افتاده است بر می‌دارد، و اگر راننده با او تصادف کند شرکت بیمه دیه دختر را پرداخت خواهد کرد. راننده چه باید بکند.

۴-۴-۲ تنازع اخلاقی قایقرانان

قایق دو قایقران A و B در دریا غرق می‌شود. تنها یک تخته در آب شناور است که توانایی شناور کردن یک نفر را دارد و اگر هر دو قایقران به تخته آویز شوند تخته به زیر آب می‌رود. قایقران A به تخته آویز می‌شود. سپس قایقران B خود را به تخته می‌رساند و به آن آویز می‌شود. قایقران A می‌بیند که تخته به زیر آب فرو می‌رود، و قایقران B را پس می‌زند. قایقران B غرق می‌شود و قایقران A به کمک یک لنج نجات پیدا می‌کند. قایقران A به آنچه در دریا اتفاق افتاده است اعتراف می‌کند. آیا قاضی می‌تواند او را به خاطر عمل نکردن به تعهدات اخلاقی و اجتماعی به قتل B متهم کند.

۵-۴-۲ تنازع بازگرداندن قرض

آقای A از دو دوست خود B و C هر کدام n میلیون تومان قرض کرده است و متعهد شده است که این پول را تا آخر دی ماه به آنها برگرداند. متأسفانه فردا آخر دی ماه است و A تنها n میلیون تومان پول دارد. هر دو دوست او در صورتی که این پول به دستشان نرسد به زندان می‌افتند. آقای A چه باید بکند.

۲-۵ همزمانی^{۲۶}

مساله همزمانی هنگامی اتفاق می افتد که چند عامل بخواهند بطور همزمان از یک منبع استفاده کنند.

۲-۵-۱ شام خوردن فیلسوفان

پنج فیلسوف دور یک میز گرد غذا خوری نشسته اند و در هنگام در حال انجام تنها یکی از دو کار زیر هستند

۱. خوردن

یا^{۲۷}

۲. فرو رفتن در اندیشه های فلسفی

بین هر دو فیلسوف مجاور یک چنگال روی میز قرار دارد. به این ترتیب هر فیلسوف یک چنگال در سمت راست خود و یک چنگال در سمت چپ خود دارد. هر فیلسوف در هنگام خوردن غذا نیاز به هر دو چنگال دو سمت خود دارد (فرض می شود که خوردن غذا با یک چنگال امکان پذیر نیست). اگر هر پنج فیلسوف بطور همزمان تصمیم به خوردن بگیرند و هر کس چنگال سمت چپ خود را بردارد، و قرار باشد هر فیلسوف منتظر نفر دست راستی خود باقی می ماند تا او چنگال را به زمین بگذارد آنگاه سیستم قفل می کند.



الگوریتم چند-عاملی زمان‌بندی برای فیلسوفان ارائه دهید بطوریکه همه فیلسوفان شام بخورند و سیستم قفل نکند.

۲-۵-۲ معمای سیگاری‌ها

.....

----- ۳-۵-۲

۲-۶ تکامل^{۲۸}

...

۲-۷ خود تنظیمی^{۲۹}

...

۲-۸ نیازها

می‌توان اینگونه فرض کرد که هر انسانی در تلاش است تا نیازهای خود را برطرف سازد و به عبارتی نیازها انسان را می‌انگیزد. وقتی نیازهای یک انسان تغییر می‌کند ترجیحات او نیز تغییر می‌کند، و در نتیجه عمل او در سیستم اجتماعی نیز تغییر می‌کند. به این ترتیب، به نظر می‌رسد در تحلیل یک سیستم اجتماعی نمی‌توان نیازهای عاملها را در نظر نگرفت. تحلیلگر سیستم اجتماعی باید از نظریه-

هایی که در مورد نیازها و انگیزه‌ها در علم روانشناسی وجود دارد آگاه باشد. هرم نیازهای مازلو، و نظریه مراحل روانی اجتماعی اریکسون از این جمله‌اند.

.....

تمرین

۱. یک مجموعه از قوانین اجتماعی حداقل باید دارای دو خصیصه سازگاری (قوانین همدیگر را نقض نکنند) و تصمیم‌پذیری (در هر وضعیتی، برای اجرا کننده، این که چه عملی را مطابق با قوانین باید (یا مجاز است) انجام دهد قابل تصمیم‌گیری است) باشد. به دفترچه قوانین حق تقدم رانندگی در ایران مراجعه کنید. به عنوان یک پروژه درسی باید بتوانید این قوانین را مدلسازی منطقی کنید و مساله تصمیم‌پذیری و سازگاری آن را مشخص کنید.
۲. قضیه Revenue Equivalence Theorem در مورد حراجی‌ها را بخوانید و مشخص کنید که در اثبات آن از چه اصول ریاضی استفاده شده است.
۳. فیلم مستند جونز تاون را ببینید و با توجه به ویژگی‌های آگاهی، تعهد، ائتلاف، رقابت و همزمانی مردم معبد، یک مقاله روزنامه ای که به دنبال توضیح کنترل اجتماعی حاکم بر مردم معبد است بنویسید. توجه کنید که این قدرت اجتماع بود که مردم معبد را پیش می‌برد نه قدرت جیم جونز.
۴. در روم باستان مجلس سنا سزار (حاکم) روم را انتخاب می‌کرد. در حالی که امپراطوری ایران اینگونه نبود. یعنی روم باستان از راهبری چندعاملی استفاده می‌کرد، در حالی که امپراطوری ایران از راهبری تکعاملی استفاده می‌کرد. چرا این تفاوت وجود داشته است؟ آیا می‌توان این تفاوت در اداره کشور را در تفاوت بین اعتقادات دینی آنها جستجو کرد؟
۵. در بخش ۱-۲، تعدادی سیستم چندعاملی را با توجه ویژگی آگاهی و تبادل آگاهی بین عامل‌ها معرفی کردیم. سعی کنید با توجه به اطرافتان سیستم‌های چندعاملی که ویژگی آگاهی در آنها نمایان است بسازید. مشخص کنید که سیستمی که معرفی کردید چه تفاوت ماهوی با سیستم‌های معرفی شده در بخش ۱-۲ دارد.

۶. پروتکل‌هایی مناسب برای بازی کارت‌های روسی معرفی کنید. سعی کنید به نحوی اثبات کنید که پروتکل شما بدون اشکال کار می‌کند.

۷. آیا می‌توانید سیستم شام خوردن ۳ رمزنگار را برای تعدادی بیشتری رمزنگار گسترش بدهید؟

۸. الگوریتمی چندعاملی برای ۴ عامل طراحی کنید که به یک تقسیم حسادت آزاد از یک منجر شود.

۹. پروتکل‌های انتخاباتی را که مساله ۲-۳-۱۱ را ارضا می‌کنند لیست کنید.

۱۰. برای آنکه در مورد تکامل و خودتنظیمی بیشتر بدانید، در اینترنت

evolution و multi agent systems+ selforganization

را جستجو کنید و نتیجه جستجو را در یک گزارش بنویسید.

مراجع

بخش ۲

مدل سازي منطقي

مروری بر منطق گزاره‌ای و محمولات

هدف این فصل مروری کوتاه بر منطق گزاره‌ای و محمولات است. فرض بر این است که خواننده با منطق آشنایی کافی دارد. مراجع [۴، ۳، ۲] را ببینید.

۳-۱ منطق گزاره‌ای

یک سیستم تبادل اطلاعات را در نظر بگیرید. می‌توان گزاره‌های زیر را در مورد سیستم بیان کرد.

۱. عامل A پیام m را به عامل B می‌فرستد.
۲. عامل C پیام m را دریافت می‌کند.
۳. پیام m بدون تغییر مخابره می‌شود.
۴. عامل A پیام m را به عامل B می‌فرستد و عامل C پیام m را دریافت می‌کند.
۵. عامل C پیام m را دریافت نمی‌کند.
۶. اگر عامل A پیام m را به عامل B می‌فرستد و پیام m بدون تغییر مخابره می‌شود آنگاه عامل C پیام m را دریافت می‌کند.
۷. عامل A پیام m را به عامل B می‌فرستد یا عامل C پیام m را دریافت می‌کند.

برای آنکه راستی گزاره‌های ۱، ۲، و ۳ را بیازماییم هیچ راهی جز مراجعه به سیستم تبادل اطلاعات مورد نظر نداریم. اما برای آنکه راستی گزاره‌های ۴، ۵، ۶ و ۷ را بیازماییم، دیگری نیازی به مراجعه به سیستم نیست و می‌توان ارزش راستی یا ناراستی آنها را با توجه به راستی و ناراستی گزاره‌های ۱، ۲، و ۳ استنتاج کرد.^{۳۰}

گزاره‌هایی چون ۱، ۲، و ۳، که برای راست آزمایی آنها مستقیم باید به سیستم مورد نظر مراجعه کرد، گزاره‌های ساده (اتمی) نامیده می‌شود. گزاره‌هایی چون ۴، ۵، ۶ و ۷ گزاره‌هایی مرکب هستند که از ترکیب گزاره‌های ساده ساخته شده‌اند.

³⁰ این موضوع از دیدگاه منطق کلاسیک برقرار است.

منطق مشخص می‌کند که چگونه از ارزش گزاره‌های ساده به ارزش گزاره‌های مرکب می‌توان پی برد.

منطق با راست آزمایی گزاره‌های مرکب سر و کار دارد، نه با راست آزمایی گزاره‌های ساده.

در این بخش مروری بسیار کوتاه به منطق گزاره‌ای می‌کنیم. برای شرح کامل حتما یکی از مراجع [۴، ۵، ۶] را ببینید.

گزاره مرکب از ترکیب گزاره‌های ساده بدست می‌آیند. ادات ترکیب عبارتند از:

▪ نقیض: گزاره ۵ نقیض گزاره ۲ است. اگر گزاره ۲ را با متغیر r نمایش دهیم. آنگاه گزاره ۵

بصورت را بصورت $\neg r$ نمایش می‌دهیم.

▪ ترکیب عطفی: گزاره ۴ عطف گزاره‌های ۱ و ۲ است. اگر q نماد گزاره ۱ و r نماد گزاره ۲

باشد، $p \wedge r$ نماد گزاره ۴ است.

▪ ترکیب فصلی: گزاره ۷ فصل گزاره‌های ۱ و ۲ است. اگر q نماد گزاره ۱ و r نماد گزاره ۲

باشد، $p \vee r$ نماد گزاره ۷ است.

▪ استلزام: در ساخت گزاره ۶ از ترکیب استلزام استفاده شده است. اگر q نماد گزاره ۱، r نماد

گزاره ۲ و p نماد گزاره ۳ باشد، $(q \wedge p) \rightarrow r$ نماد گزاره ۶ است.

۳-۱-۱ جدول ارزش‌دهی

به کمک جدول ارزش‌دهی می‌توان ارزش گزاره مرکب را با توجه به ارزش گزاره‌های ساده (اتمی) آن

مشخص کرد. در زیر جدول‌های ارزش‌دهی را برای ترکیب‌های گزاره ساز می‌بینیم.

	p	$\neg p$
$\neg$	t	f
	f	t

	p	q	$p \wedge q$
	t	t	t
$\wedge$	t	f	f
	f	t	f
	f	f	f

	p	q	$p \vee q$
	t	t	t
$\vee$	t	f	t
	f	t	t
	f	f	f

	p	q	$p \rightarrow q$
	t	t	t
$\rightarrow$	t	f	f
	f	t	t
	f	f	t

دو گزاره را هم‌ارز گوییم هرگاه برای هر ارزش‌دهی یکسان به گزاره‌های ساده ارزش آنها یکسان شود. برای مثال، $p \rightarrow q$ و $\neg p \vee q$ هم‌ارز هستند.

۳-۱-۲ بنابرین

وکیلی در یک دادگاه جنایی استدلال زیر را برای هیات منصفه ارائه می‌دهد.

اگر روز شنبه مینا تماس تلفنی نگرفته باشد یا از خانه بیرون نرفته باشد، آنگاه همسرش قاتل نیست و

قاتل واقعی لیلا است. اگر لیلا قاتل باشد شنبه شب از تهران گریخته است یا همسر مینا را ملاقات

کرده است. لیلا از تهران نگریخته است.

بنابرین،

روز شنبه مینا از خانه بیرون نرفته است.

آیا استدلال درست است؟ چگونه می‌توانیم درستی استدلال را بررسی کنیم؟

وزیر اقتصاد دیشب در برنامه تلویزیونی **رستاخیز یعنی پاسخگویی** حاضر شد و در مورد پرسش رکود

تورمی گفت:

اگر تورم افزایش پیدا کند تولید افزایش می‌یابد و اگر تولید افزایش یابد بیکاری کاهش می‌یابد. اگر انبارها خالی شود تقاضا از عرضه پیشی می‌گیرد و تورم افزایش می‌یابد. اگر مواد اولیه به کارخانه‌ها نرسد تولید نمی‌تواند افزایش یابد. انبارها خالی است و مواد اولیه به کارخانه‌ها نمی‌رسد.

بنابراین

تورم افزایش می‌یابد و بیکاری کاهش نمی‌یابد

چگونه می‌توان فهمید که وزیر اقتصاد خلاف‌گویی نمی‌کند؟

برای بررسی درستی یک استدلال دو روش وجود دارد

۱. روش جدول ارزش‌دهی

۲. روش قواعد استنتاج

که نشان داده می‌شود این دو روش در قضیه‌ای که در ادامه خواهد یکسان هستند.

روش جدول ارزش‌دهی (معناشناسی)

تعریف ۱-۲-۳

گزاره‌های $\varphi_1, \varphi_2, \dots, \varphi_n, \psi$ را در نظر بگیرید. گوییم (حکم) ψ نتیجه منطقی (فرض‌های) $\varphi_1, \varphi_2, \dots, \varphi_n$ است هرگاه برای هر ارزش‌دهی به گزاره‌های اتمی، اگر ارزش همه فرض‌ها $\varphi_1, \varphi_2, \dots, \varphi_n$ راست باشد آنگاه ارزش حکم ψ نیز راست باشد.

مثال ۳-۱-۲ با جدول ارزش‌دهی تحقیق کنید $p \wedge q$ نتیجه منطقی گزاره‌های

$$(\neg p \vee \neg q) \rightarrow (r \wedge s), r \rightarrow t, \neg t \text{ است.}$$

بیایید سخنان آقای وکیل را صورتبندی کنیم و بینیم آیا آنچه بعد از واژه *بنابراین* می‌آید نتیجه منطقی سخنان بالا آقای وکیل هست.

برای صورتبندی باید ابتدا گزاره‌های اتمی سخنان آقای وکیل را مشخص کنیم و به آنها نماد گزاره‌ای نسبت دهیم.

p : روز شنبه مینا تماس تلفنی گرفته است.

q : روز شنبه مینا از خانه بیرون رفته است.

r : همسر مینا قاتل است.

s : قاتل واقعی لیلا است.

t : لیلا شنبه شب از تهران گریخته است.

u : لیلا همسر مینا را ملاقات کرده است.

اکنون با توجه به نمادهای اتمی بالا، سخنان وکیل را صورتبندی می‌کنیم. علامت خط‌چین نمایانگر واژه *بنابراین* هست.

$$(\neg p \vee \neg q) \rightarrow (\neg r \wedge s)$$

$$s \rightarrow (t \vee u)$$

$$\neg t$$

$$\neg q$$

استدلال وکیل در صورتی درست است که گزاره زیر خط‌چین نتیجه منطقی گزاره‌های بالا خط‌چین باشد. با رسم جدول ارزش‌دهی بررسی کنید که مبدا وکیل در حال فریب هیات منصفه باشد.

تمرین ۳-۲-۱-۳ سخنان وزیر اقتصاد را صورتبندی کنید و با روش جدول ارزش‌دهی ببینید آیا او خلاف‌گویی نمی‌کند؟

روش قواعد استنتاج (دستگاه برهان)

تعریف ۴-۲-۱-۳ گزاره‌های $\varphi_1, \varphi_2, \dots, \varphi_n, \psi$ را در نظر بگیرید. گوییم (حکم) ψ از (فرض‌های) $\varphi_1, \varphi_2, \dots, \varphi_n$ قابل استنتاج است هرگاه با استفاده از تعداد متناهی از قواعد استنتاج زیر بتوان ψ را از فرض‌های $\varphi_1, \varphi_2, \dots, \varphi_n$ بدست آورد. (مفروضات می‌توانند در داخل گروه‌ها استفاده شوند)^{۳۱}

D	D	D'	D
$\varphi \wedge \psi$	$\varphi \wedge \psi$	φ	ψ
— — —	— — —	— — — —	
φ	ψ	$\varphi \wedge \psi$	

$[\varphi]$	$[\psi]$			
D'	D	D	D	
γ	γ	$\varphi \vee \psi$	φ	ψ
-----		--	--	
γ		$\varphi \vee \psi$	$\varphi \vee \psi$	

³¹ این فصل تنها مروری کوتاه بر منطق ریاضی است. برای شرح بیشتر حتمی مرجع [۴] را ببینید.

D'	D	$[\varphi]$
φ	$\varphi \rightarrow \psi$	ψ
-----		--
ψ		$\varphi \rightarrow \psi$

D'	D	$[\varphi]$
$\neg \varphi$	φ	$\perp$
-----		--
$\perp$		$\neg \varphi$

$[\neg \varphi]$	
D	D
$\perp$	$\perp$
---	---
φ	φ

مثال ۳-۱-۲-۵ گزاره $p \wedge q$ جز $(\neg p \vee \neg q) \rightarrow (r \wedge s)$ ، $r \rightarrow t$ ، $\neg t$ استنتاج کنید.

قضیه ۷-۲-۱-۳ (صحت و تمامیت) (حکم) ψ از (فرض‌های) $\varphi_1, \varphi_2, \dots, \varphi_n$ قابل استنتاج است

اگر و تنها اگر (حکم) ψ نتیجه منطقی (فرض‌های) $\varphi_1, \varphi_2, \dots, \varphi_n$ باشد.

برهان: یکی از مراجع [؟،؟،؟] را ببینید.

۲-۳ منطق محمولات

همه انسان ها فانی هستند

سقراط انسان است

پس، سقراط فانی است^{۳۲}.

استنتاج بالا ، استنتاجی ساده در زبان طبیعی است ولی آن را نمی توان در منطق گزاره ای مدل کرد.

اگر نمادهای p, q, r را به ترتیب زیر در نظر بگیریم

p : همه انسان ها فانی هستند

q : سقراط انسان است

r : سقراط فانی است.

امکان ندارد بتوان از $p \wedge q$ گزاره r را به کمک قواعد استنتاج منطق گزاره به دست آورد. در واقع،

باید زبان منطق را گسترش بدهیم تا بیشتر به زبان طبیعی نزدیک شود. به همین دلیل به زبان منطق

گزاره ای سورهای عمومی $\forall$ و وجودی $\exists$ را اضافه می کنیم.

فانی بودن یک محمول (خاصیت) است که می تواند برای قلمرویی از اشیا در نظر گرفته شود. بگذارید

برای محمول " x فانی است" نماد $P(x)$ را در نظر بگیریم و برای محمول x انسان است نماد

$H(x)$ را در نظر بگیریم. فرض کنید D یک قلمرو از اشیا باشد و $s \in D$ نمایانگر سقراط باشد.

حال با زبان محمولات می توانیم استنتاج بالا را به صورت زیر صوری سازی کنیم.

$$(\forall x \in D)(H(x) \rightarrow P(x))$$

$$H(s)$$

$$P(s)$$

³² این يك آغاز سنتي براي منطق محمولات است.

نکته: هرگاه نتوان یک استنتاج در زبان طبیعی را در زبان منطق مدل کرد، نیاز است تا زبان منطق با اضافه دشن ادات جدید گسترش یابد. منطق محمولات گسترشی از منطق گزاره‌ای است.

همانند منطق گزاره‌ای، برای منطق محمولات نیز معناشناسی و دستگاه برهان وجود دارد. (در حال حاضر فرصت کامل کردن این قسمت را ندارم برای این موضوع به یکی از مراجع [۱،۲،۳] رجوع کنید).

۳-۲-۱ پارادوکس انتخابات

در کشور خفند که **الستون** و **ولستون** در آن زندگی می‌کنند قرار است انتخابات ریاست‌جمهوری برگزار شود. حکومت از خبرنگاران خارجی دعوت کرده است تا برای تهیه گزارش از انتخابات به آن کشور سفر کنند. خبرنگار شبکه CBC در خیابان الستون را می‌بیند و از او نظرش را در مورد انتخابات می‌پرسد الستون می‌گوید:

اگر همه به آقای حبه انگور رای بدهند آنگاه حبه انگور رییس جمهور خواهد شد.

خبرنگار CBC جمله الستون را اینگونه تعبیر می‌کند که خفند کشوری دموکراتیک است و یک برنامه در مورد دموکراسی در خفند از CBC پخش می‌شود.

حکومت خفند از این برنامه استقبال می‌کند و تلویزیون‌های داخلی صحنه محاسبه آقای الستون را وقتی که جمله‌اش را می‌گوید بارها و بارها پخش می‌کنند و با اهدا سکه طلا به الستون او را مورد تشویق قرار می‌دهند.

چند روز بعد، خبرنگار یک شبکه دیگر (شبکه GCG) ولستون را در خیابان می‌بیند و از او در مورد انتخابات می‌پرسد. ولستون می‌گوید:

وجود دارد کسی که اگر او به آقای حبه انگور رای بدهد آنگاه حبه انگور رییس جمهور خواهد شد.

خبرنگار GCG جمله ولستون را اینگونه تعبیر می‌کند که خفند کشوری دیکتاتوری است که در آن کسی هست که اگر او نظرش حبه انگور باشد آنگاه حبه انگور رییس جمهور می‌شود. یک برنامه در مورد دیکتاتوری در خفند از GCG پخش می‌شود. حکومت خفند از این موضوع ناراحت می‌شود و ولستون به جرم تبلیغ علیه امنیت ملی زندانی می‌شود. اما وکیل زبردست ثابت می‌کند که ولستون همان حرفی را زده است که الستون گفته است. با منطق محمولات این موضوع را نشان دهید.

تمرین

۱. سخنان وزیر اقتصاد را صورتبندی کنید و با روش قواعد استنتاج ببینید آیا او خلاف‌گویی نمی‌کند؟
۲. یک برنامه از تلویزیون را تماشا کنید و یک جمله‌ای که در آن از واژه بنابراین (یا واژه‌ها همانند آن چون: پس، نتیجه می‌گیریم و ...) را یادداشت کنید. سپس آن را با منطق گزاره‌ای مدل کنید و هم به کمک جدول ارزشدهی و روش قواعد استنتاج درست‌یابی کنید.
۳. قضیه ۷-۲-۱-۳ می‌گوید که روش جدول ارزشدهی و روش قواعد استنتاج با هم یکسان هستند. بطور کلی به روش اول بررسی‌گر-مدل (Model Checking) و به روش دوم اثبات قضیه (Theorem Proving) می‌گویند. فرض کنید با این پرسش که آیا (حکم) ψ از (فرض‌های) $\varphi_1, \varphi_2, \dots, \varphi_n$ بدست می‌آید روبرو هستید. در روش جدول ارزشدهی، جدول را رسم می‌کنید و این برای تمام حالات ممکنه که $\varphi_1, \varphi_2, \dots, \varphi_n$ ارزش راست دارند بررسی می‌کنید که ψ نیز ارزش راست دارد یا نه. به وضوح این روش تصمیم‌پذیر است. در روش قواعد استنتاج باید یک دنباله اثبات به کمک قواعد استنتاج بسازید بطوریکه مفروضات $\varphi_1, \varphi_2, \dots, \varphi_n$ و حکم ψ باشد. آیا روش دوم تصمیم‌پذیر است؟

مراجع

[١] منطق رياضي، محمد اردشير

Dirk van Dalen, **Logic and Structure** [٢]

M. Huth and M. Ryan, **Logic in Computer Science** [٣]

منطق شناختی

منطق شناختی^{۳۳} [12,7] زبانی صوری برای توصیف آگاهی‌های هر عامل فراهم می‌کند. این منطق مفاهیم **توافق** چند عامل بر سر یک موضوع، **آگاهی توزیع شده** بین عامل‌ها را نیز به خوبی مدل می‌کند. توسیع‌های دینامیکی از منطق شناختی چون منطق اعلان عمومی^{۳۴} و منطق عمل شناختی^{۳۵} به توصیف کردن به روز رسانی آگاهی‌ها در یک سیستم چند عاملی می‌پردازند. دو نوع به روز رسانی آگاهی را برای یک سیستم چند عاملی می‌توان در نظر گرفت. یکم، به روز رسانی که یک آگاهی، در حضور همه عاملها، به اطلاع همه عاملهای سیستم می‌رسد. این نوع به روز رسانی آگاهی را **اعلان عمومی** می‌نامیم. منطق اعلان عمومی برای توصیف و استنتاج در مورد این نوع به روز رسانی کارا است. دوم، به روز رسانی که یک آگاهی فقط به یک زیر گروه از عاملها اعلان می‌شود. این نوع به روز رسانی آگاهی را **اعلان خصوصی** می‌نامیم. منطق عمل شناختی برای مدل کردن به روز رسانی نوع دوم کارا است.

۴-۱ منطق شناختی

در یک سیستم چند عاملی، آگاهی‌های هر عامل با توجه به میزان دسترسی که به اطلاعات دارد مشخص می‌شود. برای فهم این موضوع مثال زیر را در نظر بگیرید. سه کارت با رنگهای سفید w ، قرمز r و آبی b بین سه عامل با شماره های ۱، ۲ و ۳ توزیع شده است به طوریکه هر عامل تنها رنگ کارت خود را می‌بیند. به این ترتیب میزان دسترسی به اطلاعات برای عاملها متمایز است. تعداد حالت‌های ممکن که می‌تواند کارتها بین عاملها توزیع شود برابر ۶ است. هر حالت را با رشته xyz که $x, y, z \in \{r, b, w\}$ است و $x \neq y, x \neq z, y \neq z$ نشان می‌دهیم که xyz یعنی حالتی که کارت با

رنگ x در درست عامل ۱، کارت با رنگ y در دست عامل ۲، و کارت با رنگ z در دست عامل ۳ است.

I. هر عامل با توجه به میزان دسترسی که به اطلاعات دارد بین تعدادی از حالت‌های ممکن مردد است.

مثلا فرض کنید قرمز در دست عامل ۱ باشد. عامل ۱ مردد است که حالت واقعی توزیع شدن کارت‌ها آیا rbw است یا rbw .

II. یک عامل یک گزاره φ در مورد سیستم را می‌داند اگر در تمام حالت‌های ممکن که بین آنها مردد است آن گزاره درست باشد.

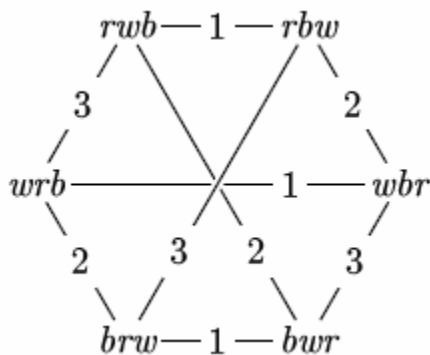
برای مثال فرض کنید حالت واقعی توزیع کارت‌ها rbw باشد. عامل ۱ نمی‌تواند بداند که

"کارت سفید دست عامل ۳ است" $:= \varphi$.

زیرا او با توجه به میزان دسترسی که به اطلاعات دارد بین حالت‌های rbw و rbw مردد است، و در حالت rbw ، کارت سفید در دست عامل ۳ نیست.

حکم‌های I و II مشخص می‌کند که چگونه یک عامل در مورد آگاهی‌های خود استدلال می‌کنند این آگاهی‌ها می‌تواند شامل آگاهی‌ها در مورد آگاهی‌های عامل‌های دیگر نیز باشد.

بازی کارت‌ها در بالا را می‌توان توسط گراف برچسب‌دار زیر مدل کرد.



هر **گره** گراف یک حالت ممکن از توزیع کارت‌ها را نمایش می‌دهد. هر **یال** گراف دارای برجستگی با نام یکی از عاملها سیستم است و وجود یال این معنا را می‌دهد که عامل مربوطه نمی‌تواند بین دو حالت ممکن که توسط یال به هم وصل شده‌اند تفاوت بگذارد. این گراف مدل کریپکی دانش^{۳۶} سیستم چند عاملی (مورد نظر) نامیده می‌شود.

برای **ساخت مدل کریپکی** یک سیستم چند عاملی، ابتدا باید برای هر حالت ممکن سیستم یک گره را در نظر گرفت. سپس با توجه به میزان دسترسی به اطلاعات هر عامل، یالهای مربوط به آن عامل را رسم کرد. توجه کنید که هر عامل هر حالت را نمی‌تواند از خود آن حالت تمیز دهد و در هر گره برای هر عامل یک طوق با برجستگی آن عامل وجود دارد که برای شلوغ نشدن گراف از ترسیم طوق‌ها صرف نظر می‌کنیم.

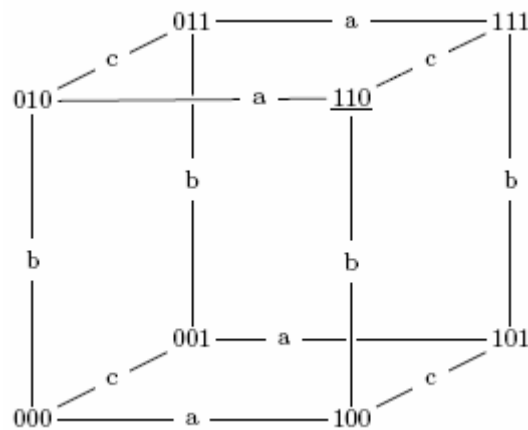
مثالی دیگر را مطالعه می‌کنیم تا ساخت مدل کریپکی برای یک سیستم چند عاملی را تمرین کنیم. فرض کنید سه کودک با نامهای a ، b و c بعد از بازی در کنار یک ساحل به خانه برمی‌گردند.

(۱) برای هر کودک این امکان وجود دارد که پیشانی او در هنگام بازی گلی شده باشد.

(۲) هر کودک فقط پیشانی دو کودک دیگر را می‌بیند و نمی‌تواند پیشانی خود را ببیند.

از جمله (۱) می‌توان حالت‌های ممکن سیستم چند عاملی را مشخص کرد. هشت حالت ممکن است. هر حالت را با رشته xyz که $x, y, z \in \{0, 1\}$ است نشان می‌دهیم که در رشته xyz ، مقدار x به کودک a ، مقدار y به کودک b و مقدار z به کودک c اشاره می‌کند و در صورتی که مقدار برابر صفر باشد یعنی پیشانی کودک مورد نظر تمیز است و در صورت ۱ بودن یعنی پیشانی کودک گلی است. برای مثال، رشته 100 یعنی پیشانی a گلی و پیشانی دو کودک دیگر تمیز است.

جمله (۲) میزان دسترسی هر عامل به اطلاعات را مشخص می‌کند. هر عامل فقط پیشانی دیگران را می‌بیند و در مورد گلی بودن یا گلی نبودن پیشانی خود مردد است. به عنوان مثال، کودک a نمی‌تواند بین دو حالت ممکن 010 و 110 تمیز قایل شود. زیرا در هر دو این حالتها گلی بودن پیشانی عاملهای دیگر یکسان است و با توجه به میزان دسترسی که a به اطلاعات کل سیستم دارد، این دو حالت یکسان هستند. گراف برجسب دار زیر مدل کریپکی این سیستم چند عاملی است.



۱-۱-۴ زبان و گرامر^{۳۷} منطق شناختی

منطق شناختی زبانی صوری را فراهم می‌کند تا بتوان دانش عاملها را بیان کرد.

تعریف ۱-۱-۴ فرض کنید P مجموعه‌ای گزاره‌های اتمی سیستم و A مجموعه عاملهای سیستم

باشد. زبان منطق شناختی $L^K(P, A)$ کوچکترین مجموعه‌ای است که

$$P \subseteq L^K(P, A) \quad \bullet$$

$$a \in A \text{ هر } \varphi, \psi \in L^K(P, A) \Rightarrow \neg\varphi, (\varphi \wedge \psi), K_a\varphi \in L^K(P, A) \quad \bullet$$

به این ترتیب، برای بدست آوردن زبان منطق شناختی، موجه دانستن (K_-) به زبان منطق گزاره‌ای^{۳۸}

اضافه می‌شود. فرمول $K_a\varphi$ بصورت زیر خوانده می‌شود

عامل a گزاره φ را می‌داند.

توجه کنید که ادات $\rightarrow, \vee$ به طور رایج در منطق گزاره‌ای از ادات $\neg, \wedge$ بدست می‌آیند.

مثال ۱-۲-۴ بازی کارتها در آغاز فصل را در نظر بگیرید. مجموعه عاملها A عبارت است از $\{1, 2, 3\}$.

مجموعه گزاره‌های اتمی P عبارت است از $\{x_i \mid x = r, w, b \text{ and } i = 1, 2, 3\}$ که فرمول x_i

معنای زیر را می‌دهد

کارت x در دست عامل i است.

اکنون برای نمونه، فرمول‌های مرکب زیر در $L^K(A, P)$ هستند.

۱. $K_1 r_1$: عامل ۱ می‌داند کارت قرمز در دست عامل ۱ است.

۲. $K_1(\neg K_2(b_3))$: عامل ۱ می‌داند که عامل ۲ نمی‌داند کارت آبی در دست عامل ۳ است.

۳. $K_2(\neg K_1(\neg r_3) \wedge \neg K_1(r_3))$: عامل ۲ می‌داند که عامل ۱ از اینکه کارت قرمز در دست عامل

۳ است بی‌اطلاع است.

برای آنکه یک سیستم چند عاملی را با منطق شناختی مورد مطالعه قرار دهیم، ابتدا باید بتوانیم گزاره-های اتمی مورد نظر را مشخص کنیم. سپس گزاره‌های مرکب که دانش عامل‌ها را توصیف^{۳۹} می‌کند قابل ساخت خواهند بود.

برای سیستم چند عاملی کودکان گلی، مجموعه عامل‌ها و گزاره‌های اتمی به این صورت است که $A = \{a, b, c\}$ و $P = \{m_a, m_b, m_c\}$ که m_j ($j = a, b, c$) یعنی

کودک با نام j گلی است.

اکنون جمله‌ای چون "کودک a می‌داند که کودک b می‌داند که آیا کودک a گلی است یا نه" با گزاره مرکب $K_a(K_b m_a \vee K_b \neg m_a)$ توصیف می‌شود.

۴-۱-۲ معناشناسی^{۴۰} منطق شناختی

در بخش قبل به این پرداختیم که چگونه در منطق شناختی به وسیله گزاره‌های اتمی سیستم می‌توان گزاره‌های مرکب ساخت. اکنون می‌خواهیم در مورد مفهوم درستی یک گزاره، و این یک گزاره در چه

شرایطی صادق است صحبت کنیم. درستی یک گزاره φ ، مرتبط به یک سیستم چند عاملی، در مدل کریپکی دانش آن سیستم چند عاملی مشخص می‌شود.

تعریف ۳-۱-۴ یک مدل کریپکی M برای یک سیستم چند عاملی با مجموعه عاملهای A و با مجموعه گزاره‌های اتمی P ، چند تایی

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

است که

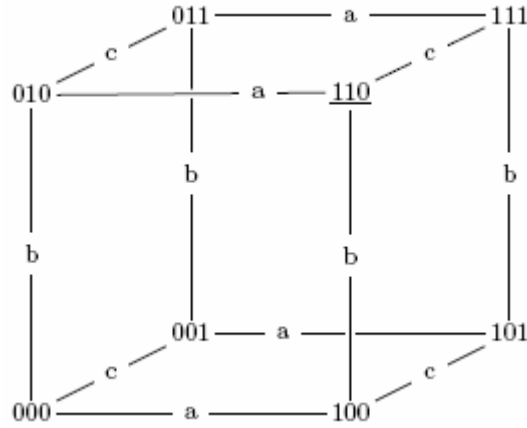
- S مجموعه همه حالت‌های ممکن سیستم است،
 - $\pi : S \rightarrow 2^P$ تابعی است که به هر حالت ممکن یک زیر مجموعه از P را نسبت می‌دهد که برای هر $s \in S$ ، عبارت $\pi(s)$ تمام گزاره‌های اتمی است که در حالت s درست هستند، و
 - برای هر عامل $a \in A$ ، $R_a \subseteq S \times S$ رابطه‌ای بین حالت‌ها است که مشخص می‌کند عامل a با توجه به میزان دسترسی‌اش به اطلاعات سیستم، چه حالت‌هایی را نمی‌تواند از هم تمیز دهد.
- برای هر $s \in S$ ، زوج (M, s) یک مدل نقطه‌ای^{۴۱} دانش نامیده می‌شود. برقراری^{۴۲} (ارضا شدن) یک گزاره $\varphi \in L(A, P)$ در مدل نقطه‌ای (M, s) با نماد $(M, s) \models \varphi$ نمایش داده می‌شود و با نگاه به ساختار φ به صورت زیر تعریف می‌گردد.

$$\begin{aligned}
(M, s) \models p & \quad \text{iff } p \in \pi(s) \\
(M, s) \models (\varphi \wedge \psi) & \quad \text{iff } (M, s) \models \varphi \text{ and } (M, s) \models \psi \\
(M, s) \models \neg \varphi & \quad \text{iff } \text{not } (M, s) \models \varphi \\
(M, s) \models K_a \varphi & \quad \text{iff for all } t \text{ such that } R_a(s, t), (M, t) \models \varphi
\end{aligned}$$

می‌گوییم گزاره φ در مدل کریپکی M برقرار است (ارضا می‌شود) هرگاه برای هر $s \in S$ داشته

$$(M, s) \models \varphi \text{ باشیم}$$

مثال ۴-۱-۴ مدل کریپکی سیستم چند عاملی کودکان گلی را در نظر بگیرید.



مجموعه همه حالت‌های ممکن $S = \{xyz \mid x, y, z = 0, 1\}$ است.

برای هر حالت $s = xyz$ که $x, y, z \in \{0, 1\}$ تابع π بصورت زیر تعریف می‌شود

$$m_a \in \pi(xyz) \Leftrightarrow x = 1$$

$$m_b \in \pi(xyz) \Leftrightarrow y = 1$$

$$m_c \in \pi(xyz) \Leftrightarrow z = 1$$

برای مثال $\pi(011) = \{m_b, m_c\}$ و $\pi(010) = \{m_b\}$ است.

رابطه‌های تمیزناپذیری بین عاملها نیز بصورت زیر است

$$R_a = \{(x_0y_0z_0, x_1y_1z_1) \mid y_0 = y_1, z_0 = z_1\}$$

$$R_b = \{(x_0y_0z_0, x_1y_1z_1) \mid x_0 = x_1, z_0 = z_1\}$$

$$R_c = \{(x_0y_0z_0, x_1y_1z_1) \mid y_0 = y_1, x_0 = x_1\}$$

اکنون با توجه به تعریف "ارضا شدن" خواننده می‌تواند برای نمونه برقراری‌های زیر را بررسی کند.

$$(M, 011) \models K_a m_c$$

$$(M, 011) \models K_a K_c m_b$$

$$(M, 011) \models K_a (K_b(m_a) \vee K_b(\neg m_a))$$

$$(M, 011) \models \neg(K_b(m_b) \vee K_b(\neg m_b))$$

در واقع برقراری‌های بالا این موضوع را بیان می‌کنند که اگر 011 حالت واقع شده باشد آنگاه گزاره‌های

سمت راست نماد $\models$ در مورد آگاهی‌های عامل‌ها برقرار هستند.

تمرین. آذر و باران روبروی هم نشسته‌اند. هر عامل روی پیشانی عامل دیگر عددی طبیعی را می‌بیند.

این دو عدد پشت‌سرهم (متوالی) هستند. هر دو عامل از متوالی بودن دو عدد آگاهند و از آگاهی

همدیگر بر این موضوع آگاهند و

۱. مدل کریپکی را برای این سیستم دوعاملی رسم کنید.

۲. مجموعه گزاره‌های اتمی سیستم را مشخص کنید.

۳. برای دو جهان ممکن از مدل، چند فرمول بنویسید که در این جهان ارضا شوند.

۴-۱-۳ اصول منطق شناختی

با توجه به اینکه چه اصولی را برای منطق شناختی در نظر بگیریم منطق دانش S5 یا منطق باور KD45 را خواهیم داشت.

A1. همه گزاره‌های همانگویی منطق گزاره به عنوان اصول در نظر گرفته می‌شوند

A2. $K_i\varphi \wedge K_i(\varphi \rightarrow \psi) \rightarrow K_i\psi$ دانش (یا باور) نسبت به استنتاج بسته است.

A3. $K_i\varphi \rightarrow \varphi$ اگر عاملی گزاره‌ای را بداند آنگاه آن گزاره صادق است.

A4. $K_i\varphi \rightarrow K_iK_i\varphi$ اگر عاملی گزاره‌ای را بداند آنگاه می‌داند که آن گزاره را می‌داند.

A5. $\neg K_i\varphi \rightarrow K_i\neg K_i\varphi$ اگر عاملی گزاره‌ای را نداند آنگاه می‌داند که آن گزاره را نمی‌داند.

همچنین دو قاعده استنتاج زیر نیز در نظر گرفته می‌شود.

$$\frac{\varphi \quad \varphi \rightarrow \psi}{\psi} \text{.R1}$$

$$\frac{\varphi}{K_i\varphi} \text{.R2}$$

منطق دانش S5 عبارت از ۵ اصل فوق همراه با دو قاعده استنتاج R1 و R2 می‌باشد. اگر به جای اصل

A3، اصل زیر را در نظر بگیریم منطق باور KD45 بدست می‌آید.

D. $\neg(K_i\varphi \wedge K_i\neg\varphi)$ باور هر عامل سازگار است.

اگر در یک مدل کریپکی اصل A3 برقرار باشد $K_i\varphi$ را اینگونه می‌خوانیم که "عامل i گزاره φ را می‌داند"، و اگر تنها اصل D برقرار باشد $K_i\varphi$ را اینگونه می‌خوانیم که "عامل i گزاره φ را باور دارد". رابطه بین اصول و مدل‌های کریپکی بصورت زیر است.

اصل A3 در یک مدل کریپکی برقرار است اگر و تنها اگر روابط تمیز ناپذیری عامل‌ها خاصیت بازتابی داشته باشند. برای هر عامل i و هر حالت $s \in S$ ، $(s, s) \in R_i$ است. یعنی هر عامل هر حالت سیستم را نتواند از خود آن حالت تمیز دهد.

اصل A4 در یک مدل کریپکی برقرار است اگر و تنها اگر روابط تمیز ناپذیری عامل‌ها خاصیت تراگذاری داشته باشند. . برای هر عامل i ، $(s, t) \in R_i \ \& \ (t, u) \in R_i \Rightarrow (s, u) \in R_i$.

اصل A5 در یک مدل کریپکی برقرار است اگر و تنها اگر روابط تمیز ناپذیری عامل‌ها خاصیت اقلیدسی داشته باشند. . برای هر عامل i ، $(s, t) \in R_i \ \& \ (s, u) \in R_i \Rightarrow (t, u) \in R_i$.

اصل D در یک مدل کریپکی برقرار است اگر و تنها اگر روابط تمیز ناپذیری عامل‌ها خاصیت سریالی داشته باشند. . برای هر عامل i ، $(\forall s \in S)(\exists t \in S) (s, t) \in R_i$.

به رابطه‌ای که خاصیت بازتابی، تراگذاری و اقلیدسی را دارد رابطه S5 گوییم.

توجه: از این بعد، همه رابطه‌های تمیز ناپذیری S5 خواهند بود.

تعریف ۴-۱-۵ برای دو گزاره $\varphi, \psi \in L(A, P)$ ، گوییم φ, ψ هم‌ارزش هستند ($\varphi \equiv \psi$) هرگاه

برای هر مدل نقطه‌ای (M, s) ، داشته باشیم

$$(M, s) \models \varphi \quad \text{iff} \quad (M, s) \models \psi$$

تمرین. با دلیل تحقیق کنید که کدامیک از هم‌ارزی‌های زیر صحیح است.

$$K_a(\varphi \wedge \psi) \equiv K_a\varphi \wedge K_a\psi$$

$$K_a(\varphi \vee \psi) \equiv K_a\varphi \vee K_a\psi$$

$$K_a(\varphi \rightarrow \psi) \equiv K_a\varphi \rightarrow K_a\psi$$

$$K_a(\neg\varphi) \equiv \neg K_a\varphi$$

تعریف ۴-۱-۶ گزاره $\varphi \in L(A, P)$ را راستگو گوییم هرگاه برای هر مدل نقطه‌ای (M, s) ، داشته

باشیم $(M, s) \models \varphi$.

تمرین. با دلیل تحقیق کنید که آیا گزاره‌های زیر راستگو هستند

$$K_a K_b \varphi \rightarrow K_a \varphi$$

$$K_a \varphi \vee K_a \neg \varphi$$

۴-۲ دانش گروهی

از سه نوع دانش گروهی می‌توان نام برد

۱. همه دانی^{۴۳}: گوییم گزاره φ یک همه دانی بین مجموعه همه عاملها در B است هرگاه هر

عامل $b \in B$ گزاره φ را بداند. همه دانی φ بین عاملها در B را با نماد $E_B\varphi$ نشان می‌دهیم

$$E_B\varphi := \bigwedge_{b \in B} K_b\varphi \text{ و}$$

فرض کنید یک گروه امنیتی پلیس ۵ مامور دارد و هر ۵ مامور در خانه خود در حال استراحت هستند. مرکز بوسیله تلفن به هر مامور خبر می‌دهد که

"جان هر ۵ نفر گروه در خطر است": φ .

اکنون هر مامور پلیس گزاره φ را می‌داند و φ یک همه دانی است. اما هر مامور پلیس مردد است که آیا همکاران دیگر او نیز φ را می‌دانند.

۲. همه دانی مشترک^{۴۴}: گوییم گزاره φ یک همه دانی مشترک بین مجموعه همه عاملها در B

است هرگاه همه عاملها در B با هم گزاره φ را بدانند. یعنی هر عاملی در B گزاره φ را

بداند و هر عامل بداند که همه عاملها φ را می‌دانند و هر عامل بداند که همه عاملها می‌دانند

که همه عاملها φ را می‌دانند و ... همه دانی مشترک φ بین عاملها در B را با نماد $C_B\varphi$

$$\text{نشان می‌دهیم و } C_B\varphi := E_B\varphi \wedge E_BE_B\varphi \wedge E_BE_BE_B\varphi \wedge \dots$$

در پروتکل‌های اجتماعی با مفهومی به نام توافق^{۴۵} روبرو می‌شویم. به طوریکه می‌خواهیم بعد از انجام پروتکل، چند عامل در مورد یک اطلاع با هم توافق داشته باشند. مثلاً در یک پروتکل احراز اصالت، می‌خواهیم دو عامل در مورد هویت یکدیگر توافق داشته باشند. یا در یک پروتکل توزیع کلید رمزنگاری، می‌خواهیم یک کلید رمزنگاری k به عنوان کلید مشترک بین دو عامل توزیع شود و عاملها بر سر کلید k توافق داشته باشند. یا در نظریه بازی‌ها عامل‌ها روی سود هر بازیکن از انجام استراتژی‌ها مختلف در بازی توافق دارند. این توافق چیزی جز همان همه دانی مشترک نیست.

۳. دانش توزیع شده^{۴۶}: گوییم گزاره φ یک دانش توزیع شده بین مجموعه همه عاملها در B است هرگاه همه عاملها در B با کنار هم گذاشتن دانش‌هایشان گزاره φ را بدانند. دانش توزیع شده را با $D\varphi$ نمایش می‌دهیم.

مفهوم دانش توزیع شده همانند یک پازل دانش است، که هر تکه پازل می‌تواند در دست یک عامل باشد. عامل‌های با کنار هم قرار دادن تکه‌های پازل خود می‌توانند دانش توزیع شده را استنتاج کنند.

مفهوم همه‌دانی مشترک به معنای توافق از اهمیت زیادی برخوردار است. شاید بتوان گفت که اگر در مورد یک موضوع در یک پروتکل امنیت همه دانی مشترک بین عاملها اتفاق نیفتد همواره راه نفوذی برای دشمن وجود دارد. مثال زیر اهمیت این مفهوم را آشکارتر می‌کند.

مثال ۴-۲-۱ فرض کنید دو فرمانده متحد a, b همراه با لشگرهایشان روی دو قله کوه، که در دره بین دو قله لشگر دشمن قرار دارد، کمین کرده‌اند. اگر هر دو سردار همزمان به دشمن حمله کنند پیروز می‌شوند و اگر در زمانهای متفاوت حمله کنند شکست خواهند خورد. فرمانده a پیکی را با پیام زیر برای فرمانده b می‌فرستد.

فردا صبح هنگام طلوع به دشمن حمله کنیم: φ

پیک مجبور است دره بین دو قله را رد کند و همیشه احتمال اینکه به دست دشمن اسیر شود هست.

فرض کنید پیک بتواند به سلامت دره را رد کند. در این صورت داریم

$$K_a\varphi \wedge K_bK_a\varphi$$

یعنی فرمانده a گزاره φ را می‌داند و فرمانده b نیز می‌داند که فرمانده a گزاره φ را می‌داند. آیا

فرمانده‌ها حمله می‌کنند؟ خیر، توافقی (همه‌دانی مشترکی) بین فرمانده‌ها اتفاق نیفتاده است. فرمانده

a این حالت را ممکن می‌داند که پیک نتوانسته باشد به سلامت دره را رد کند. یعنی فرمانده a نیم-

داند که فرمانده b گزاره φ را می‌داند

$$\neg K_aK_b\varphi$$

حال فرض کنید فرمانده b از پیک می‌خواهد برگردد و خبر رسیدن پیام را به فرمانده خود بدهد.

فرض کنید باز هم پیک به سلامت دره را رد کند. خواهیم داشت

$$K_aK_b\varphi \wedge K_bK_a\varphi$$

آیا فرمانده‌ها حمله می‌کنند؟ خیر، باز هم توافقی (همه‌دانی مشترکی) بین فرمانده‌ها اتفاق نیفتاده

است. فرمانده b این حالت را ممکن می‌داند که پیک نتوانسته باشد به سلامت دره را رد کند. یعنی

$$\neg K_bK_aK_b\varphi$$

به این ترتیب، باز فرمانده a مجبور است دوباره پیک را به سمت b راهی کند و هیچگاه نمی‌توانند

فرمانده‌ها به توافق برسند یعنی $C_{\{a,b\}}\varphi$ هیچگاه برقرار نمی‌شود.

برای توصیف همه‌دانی مشترک و دانش توزیع شده دو موجه C_B و D_B را به زبان منطق شناختی اضافه می‌کنیم. معناشناسی این دو موجه در یک مدل کریپکی دانش به صورت زیر در نظر گرفته می‌شود.

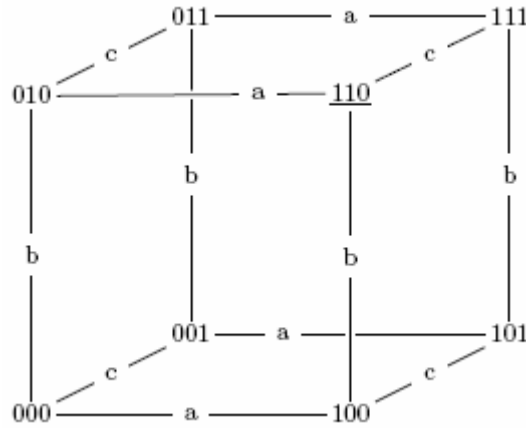
• $(M, s) \models C_B \varphi$ اگر و تنها اگر برای هر حالت t در مدل، که مسیری از s به t (با یالهای

برچسب دار از مجموعه B) وجود دارد، داشته باشیم $(M, t) \models \varphi$.

• $(M, s) \models D_B \varphi$ اگر و تنها اگر برای هر حالت t در مدل، که $(s, t) \in \cap_{b \in B} R_b$ ، داشته باشیم

$(M, t) \models \varphi$.

مثال ۲-۲-۴ مدل کریپکی دانش مساله کودکان گلی را در نظر بگیرید.



فرمول

"حد اقل یکی از کودکان گلی است" $\psi :=$

را در نظر بگیرید. داریم

$$(M, 110) \models K_c E_{\{a, b, c\}} \psi \wedge \neg K_b E_{\{a, b, c\}} \psi \wedge \neg K_c E_{\{a, b, c\}} \psi$$

یعنی اگر 110 حالت واقع باشد، آنگاه همه کودکان (با توجه به میزان دسترسی آنها به اطلاعات) می-
 دانند که حداقل یک نفر پیشانی‌اش گلی است. اما کودک c می‌داند که همه می‌دانند که پیشانی
 حداقل یک نفر گلی است در حالیکه کودک b و کودک c این را نمی‌دانند. پس ψ همه‌دانی مشترک
 نیست

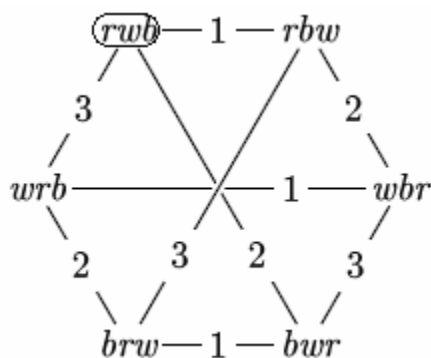
$$(M, 110) \models \neg C_{\{a,b,c\}} \psi$$

می‌توان این موضوع را که ψ همه‌دانی مشترک نیست با توجه به تعریف معناشناسی همه‌دانی مشترک
 در مدل‌های کریپکی نیز به این روش بررسی کرد که مسیری (فارغ از برچسب‌ها) از حالت 110 به
 حالت 000 در گراف مدل کریپکی موجود است و در حالت 000 گزاره ψ برقرار نیست.

۳-۴ منطق اعلان عمومی

در یک سیستم چند عاملی ساده‌ترین راهی که سبب می‌شود اطلاعات عاملها تغییر کند این است که یک اطلاع صادق در حضور همه عاملها به طور عمومی اعلان شود. فرض کنید عاملهای A همه با هم در یک اتاق حضور داشته باشند. گزاره ψ برای اعضای A اعلان عمومی^{۴۷} می‌شود، هرگاه ψ در حضور همه اعضا با صدای بلند بیان شود. با اعلان عمومی یک گزاره میزان دسترسی عاملها به اطلاعات سیستم تغییر می‌کند. به این ترتیب مدل کریپکی دانش سیستم چند عاملی باید به روز رسانی^{۴۸} شود. در این بخش به این می‌پردازیم که چگونه این بروز رسانی انجام می‌شود. منطق اعلان عمومی این امکان را فراهم می‌کند تا بتوان در مورد آگاهی‌های عاملها بعد از اعلان عمومی در یک سیستم چند عاملی استدلال کرد.

سیستم چند عاملی بازی کارتها را که در بخش ۳-۱ معرفی شد در نظر بگیرید. فرض کنید حالت واقع توزیع کارتها rbw باشد. همانطور که قبلاً توضیح داده شد، هر عامل فقط کارت خود را می‌بیند و با توجه به این گونه دسترسی از اطلاعات، مدل کریپکی دانش سیستم به صورت زیر است (حالت واقع را در شکل در داخل یک بیضی قرار دادیم).

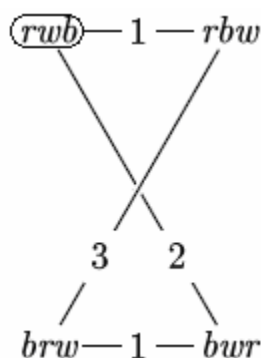


$M1$: مدل آغازین

فرض کنید اعلان عمومی به این ترتیب اتفاق افتد که در حضور همه اعضا بلند گفته شود

"کارت سفید در دست عامل ۱ نیست" ψ_1

قبل از این اعلان عمومی، عامل‌های ۶ حالت را برای سیستم ممکن می‌دانستند و هر عامل با توجه به میزان دسترسی‌اش به اطلاعات بین حالت‌ها مختلف تردد بود (مدل بالا). بعد از اعلان عمومی ψ_1 ، همه عامل‌ها می‌فهمند که حالت واقع یکی از حالت‌هایی که سفید در دست عامل اول باشد نیست، یعنی حالت واقع، هیچکدام از حالت‌های wrb و wbr نیست. پس دیگر، عامل‌ها این دو حالت را به عنوان حالت‌هایی از سیستم در نظر نمی‌گیرند و فقط ۴ حالت را پس از اعلان عمومی برای سیستم مجاز می‌شمارند یعنی حالت‌های rbw, rbw, brw, bwr . عامل‌ها تنها بین این ۴ حالت تردد هستند و مدل کریپکی دانش پس از اعلان ψ_1 به صورت زیر بروز رسانی خواهد بود.



$M2$: مدل حاصل از به روز رسانی $M1$ با اعلان عمومی ψ_1

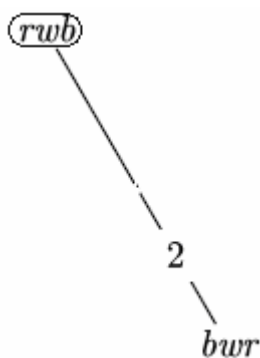
در مدل جدید، عامل ۳ در مورد اینکه حالت واقع کدام حالت است تردد نیست (هیچ یالی با برچسب ۳ حالت واقع را به حالتی غیر از خود حالت واقع متصل نمی‌کند). عامل ۳ پس از اعلان عمومی از نحوه

توزیع کارتها مطلع است. اما عاملهای ۱ و ۲ هنوز از نحوه توزیع کارتها مطلع نیستند عامل ۲ می‌داند که عامل ۳ توزیع کارتها را می‌داند ولی عامل ۱ این را نمی‌داند.

حال، فرض کنید اعلان عمومی دومی به این صورت اتفاق افتد که در حضور همه اعضا بلند گفته شود

"عامل ۲ هنوز نمی‌داند که کارت نفر اول چیست" ψ_2

بعد از این اعلان، عاملها می‌فهمند که هیچکدام از حالت‌های rbw و brw حالت واقع سیستم نبوده‌اند زیرا در هر دو این حالتها عامل ۲ می‌داند که کارت نفر اول چیست. پس دیگر، عاملها این دو حالت را به عنوان حالت‌هایی از سیستم در نظر نمی‌گیرند و مدل کریپکی دانش به صورت زیر به روز رسانی می‌شود.



$M3$: مدل حاصل از به روز رسانی $M2$ با اعلان عمومی ψ_2

در حالت $(M3, rbw)$ هر دو عامل ۱ و ۳ از نحوه توزیع کارتها مطلع‌اند اما عامل ۲ هنوز نحوه توزیع کارتها را نمی‌داند. دقت کنید که عامل ۲ بعد از این درو به روز رسانی می‌داند که دو عامل دیگر از نحوه توزیع کارتها مطلع‌اند.

منطق اعلان عمومی این امکان را فراهم می‌کند که بتوانیم در مورد آگاهی‌های عاملها بعد از اعلان‌های عمومی استدلال کنیم.

۱-۳-۴ زبان و گرامر منطق اعلان عمومی

تعریف ۱-۳-۳ فرض کنید P مجموعه‌ای گزاره‌های اتمی سیستم و A مجموعه عامل‌های

سیستم باشد. زبان منطق اعلان عمومی $L^{\perp}(P, A)$ کوچکترین مجموعه‌ای است که

$$P \subseteq L^{\perp}(P, A) \quad \bullet$$

$$a \in A \Rightarrow \neg\varphi, (\varphi \wedge \psi), K_a\varphi, [\varphi]\psi \in L^{\perp}(P, A)$$

که عملگر $[\varphi]$ عملگر اعلان عمومی (برای گزاره φ) است، و فرمول $[\varphi]\psi$ به صورت زیر خوانده می‌شود

"بعد از اعلان عمومی φ ، گزاره ψ برقرار می‌گردد."

برای مثال، در بازی کارتها می‌توان گزاره‌های زیر را در زبان منطق اعلان عمومی نمایش داد

$$\bullet \quad [\neg w_1](K_3w_1 \vee K_3r_1 \vee K_3b_1)$$

نیست، عامل ۳ می‌داند که چه کارتی در دست عامل ۱ است.

$$\bullet \quad [\neg w_1][\neg(K_2w_1 \vee K_2r_1 \vee K_2b_1)](K_1w_3 \vee K_1r_3 \vee K_1b_3)$$

سفید در دست عامل ۱ نیست و اعلان عمومی اینکه عامل ۲ هنوز نمی‌داند چه کارتی در

دست عامل ۱ است، عامل ۱ می‌داند که کارت عامل ۳ چیست.

۲-۳-۴ معناشناسی منطق اعلان عمومی

برای یک مدل نقطه‌ای (M, s) باید مشخص کنیم که فرمول‌هایی به صورت $[\varphi]\psi$ در چه صورت در

(M, s) ارضا می‌شوند.

تعریف ۴-۳-۲ گزاره $[\varphi]\psi$ در مدل نقطه‌ای (M, s) ارضا می‌شود، $(M, s) \models [\varphi]\psi$ ، هرگاه

اگر $(M, s) \models \varphi$ آنگاه $(M, s) \models \psi$.

مدل $M_{|\varphi} = \langle S_{|\varphi}, \pi_{|\varphi}, (R_{a|\varphi})_{a \in A} \rangle$ از روی مدل $M = \langle S, \pi, (R_a)_{a \in A} \rangle$ به صورت زیر ساخته می‌شود.

$$S_{|\varphi} = \{s \in S \mid (M, s) \models \varphi\}$$

$$\pi_{|\varphi} = \pi \mid S_{|\varphi}$$

$$R_{a|\varphi} = R_a \mid S_{|\varphi}$$

مدل $M_{|\varphi}$ از روی مدل M به این ترتیب ساخته می‌شود که از همه حالت‌هایی که در آنها φ ارضا نمی‌شود صرف‌نظر می‌کنیم. سپس تابع $\pi_{|\varphi}$ و روابط $R_{a|\varphi}$ با تحدید کردن تابع π و روابط R_a به مجموعه حالت‌های باقیمانده ساخته می‌شوند.

به این ترتیب، برای آنکه بررسی کنیم آیا بعد از اعلان عمومی φ گزاره ψ برقرار می‌گردد (یعنی، $(M, s) \models [\varphi]\psi$)، باید مدل دانش را با توجه به گزاره φ به روز رسانی کرده و در مدل جدید درستی گزاره ψ را بررسی کنیم (یعنی $(M_{|\varphi}, s) \models \psi$).

برای نمونه، مدل‌های $M1$ ، $M2$ و $M3$ بازی کارتها در بالا را در نظر بگیرید. داریم

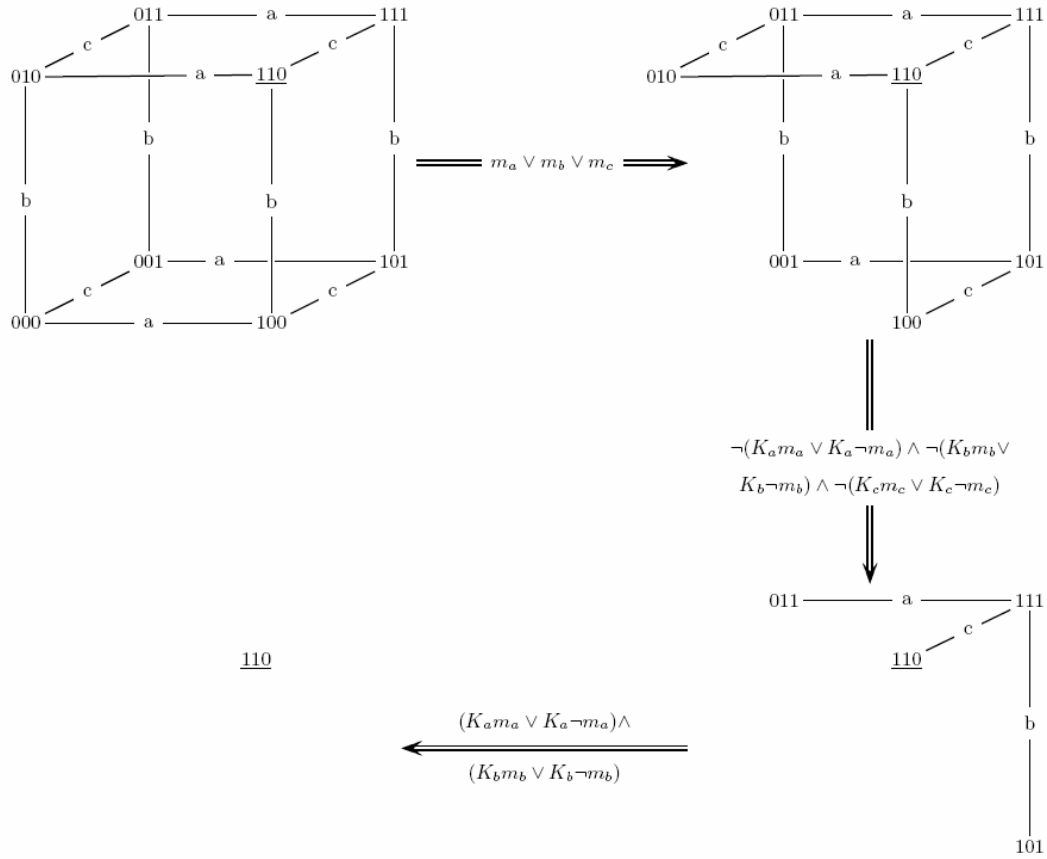
$$M2 = M1_{|\neg w_1}$$

$$M3 = M2_{|\neg(K_2 w_1 \vee K_2 r_1 \vee K_2 b_1)}$$

با توجه به تعریف معناشناسی داریم $(M1, rwb) \models [\neg w_1]K_3 r_1$ زیرا $(M2, rwb) \models K_3 r_1$. همچنین،

$$(M3, rwb) \models K_1 b_3 \text{ زیرا } (M1, rwb) \models [\neg w_1][\neg(K_2 w_1 \vee K_2 r_1 \vee K_2 b_1)]K_1 b_3$$

تمرین. مساله کودکان گلی را به کمک منطق اعلان عمومی مدل کنید.



تمرین. با دلیل تحقیق کنید که آیا گزاره‌های زیر راستگو هستند

$$[\varphi](\psi \wedge \chi) \leftrightarrow ([\varphi]\psi \wedge [\varphi]\chi)$$

$$[\varphi](\psi \rightarrow \chi) \leftrightarrow ([\varphi]\psi \rightarrow [\varphi]\chi)$$

$$[\varphi](\neg\psi) \leftrightarrow (\varphi \rightarrow \neg[\varphi]\psi)$$

$$[\varphi]K_i\psi \leftrightarrow (\varphi \rightarrow K_i[\varphi]\psi)$$

$$[\varphi][\psi]\chi \leftrightarrow [\varphi \wedge [\varphi]\psi]\chi$$

مثال ۳-۳-۴ پارادوکس کلانتر.

۵ نفر پشت سر هم در یک صف ایستاده‌اند بطوریکه هر نفر تنها پشت نفرات جلویی خود را می‌بیند.



فرماندار یک ستاره طلایی در دست دارد که این ستاره را به پشت لباس یکی از افراد می‌چسباند تا کلانتر محل را مشخص کند. سپس فرماندار اعلام می‌کند

در پشت سر تنها یکی از شما ستاره طلایی چسبانده شده است، ولی آن فرد از این موضوع مطلع نیست

مدل‌سازی مساله برای دو عامل:

I. یک مدل‌سازی نادرست:

در مدل‌سازی زیر همه جهان‌های ممکن در نظر گرفته نشده‌اند، همچنین اعلان عمومی فرماندار به طور صحیح توصیف منطقی نشده است.

دو عامل 1,2 را در نظر بگیرید. که عامل 2 پشت سر عامل 1 ایستاده است. سیستم چند عاملی مساله به صورت زیر است.

۱. $A = \{1, 2\}$ مجموعه عاملها و

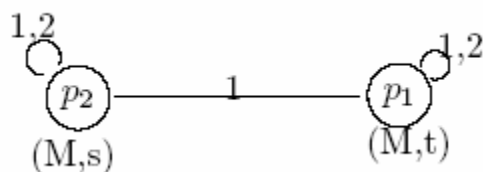
۲. $P = \{p_1, p_2\}$ مجموعه اتمی‌ها که

عامل i در پشت لباسش ستاره نصب شده است p_i

مدل کریپکی سیستم چند عاملی بصورت زیر است.

۱. دو جهان ممکن قابل تصور است.

۲. روابط بین جهان های ممکن با توجه به دسترسی عامل ها به اطلاعات سیستم (دیدن عاملها) مشخص می شود.



چون عامل 1 نمی تواند پشت سر عامل 2 را ببیند به همین دلیل بین دو حالت (M,s) و (M,t) نمی تواند تمییز قایل شود.

اعلان عمومی فرماندار به صورت زیر توصیف می شود.

$$[(p_1 \rightarrow \neg K_1 p_1) \wedge (p_2 \rightarrow \neg K_2 p_2)]$$

II. مدل سازی درست:

دو عامل 1,2 را در نظر بگیرد. که عامل 2 پشت سر عامل 1 ایستاده است. سیستم چند عاملی مساله به صورت زیر است.

۳. $A = \{1,2\}$ مجموعه عاملها و

۴. $P = \{p_1, p_2\}$ مجموعه اتمی ها که

عامل i در پشت لباسش ستاره نصب شده است p_i

مدل کریپکی سیستم چند عاملی بصورت زیر است.

۳. چهار جهان (حالت) ممکن قابل تصور است.

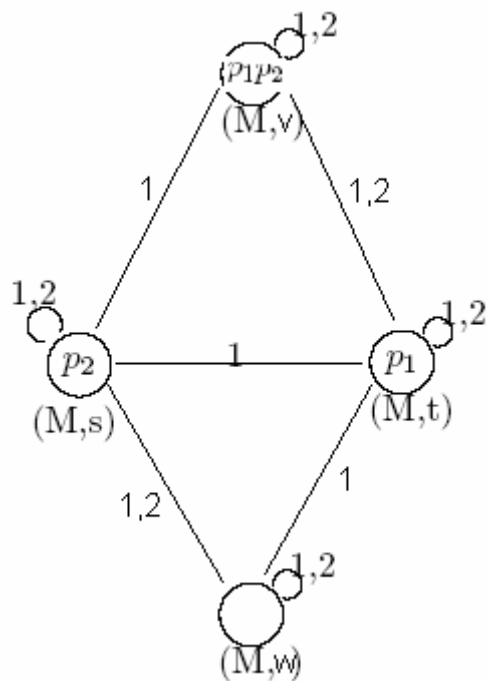
a. جهانی که پشت سر هیچکس ستاره ای چسبیده نباشد.

b. جهانی که پشت سر هر دو ستاره ای چسبیده باشد

c. جهانی که تنها پشت سر عامل ۱ ستاره چسبیده باشد

d. جهانی که تنها پشت سر عامل ۲ ستاره چسبیده باشد

۴. روابط بین جهان های ممکن با توجه به دسترسی عامل ها به اطلاعات سیستم (میدان دید عاملها) مشخص می شود.



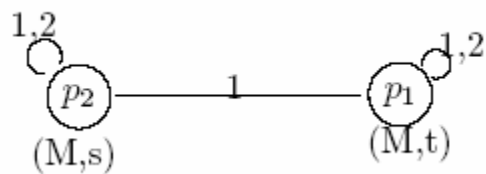
چون عامل 1 نمی تواند پشت سر عامل 2 را ببیند به همین دلیل بین هر چهار حالت نمی تواند تمییز قایل شود. اما عامل ۲ می تواند بین بعضی از حالتها تمییز قایل شود

حال نوبت فرماندار است که یک جهان ممکن را با چسباندن ستاره به جهان واقع تبدیل کند. و سپس اعلان عمومی کند.

اعلان عمومی فرماندار به صورت زیر توصیف می شود.

$$[(p_1 \vee p_2) \wedge \neg(p_1 \wedge p_2) \wedge (p_1 \rightarrow \neg K_1 p_1) \wedge (p_2 \rightarrow \neg K_2 p_2)]$$

بعد از اعلان عمومی فوق مدل به روز رسانی شده بصورت زیر است:



یعنی هنوز بعد از اعلان عمومی فرماندار دو جهان ممکن (M, s) و (M, t) هستند که می توانند جهان واقع باشند آیا پارادوکس از این موضوع بر می خیزد؟

۴-۴ عمل شناختی

در بخش قبل، گفتیم ساده‌ترین نوع تغییر اطلاعات در یک سیستم چند عاملی آن است که یک خبر در حضور همه عاملها اعلان عمومی شود. در برابر اعلان عمومی می‌توان اعلان خصوصی^{۴۹} را در نظر گرفت، به این ترتیب که یک خبر فقط در یک زیرگروه از عاملها اعلان عمومی می‌شود و عاملهایی که در زیر گروه نیستند در مورد این که چه خبری اعلان عمومی شده است مردد هستند. در این بخش، با معرفی کردن عملهای شناختی به مدل کردن اعلان‌های خصوصی می‌پردازیم.

دو دوست با نامهای a و b در اتاق نشیمن دور یک میز که یک پاکت نامه روی آن قرار دارد نشسته‌اند. نامه در مورد خبر قبولی a در دانشگاه است و هر دو دوست می‌دانند که در نامه یا خبر

$$p := "a \text{ در دانشگاه قبول شده است}"$$

یا خبر

$$\neg p := "a \text{ در دانشگاه قبول نشده است}"$$

نوشته شده است. مدل کریپکی دانش عاملها به صورت زیر است.

0	—————	a, b	—————	$\frac{1}{t1}$
t2				t1

M

سیستم دارای دو حالت ممکن است، که حالت 0 (حالت t_2) حالتی است که روی نامه $\neg p$ نوشته شده باشد و حالت 1 (حالت t_1) حالتی است که روی نامه p نوشته شده باشد. از آنجا که نامه داخل پاکت است هر دو عامل a و b بین دو حالت ممکن مردد هستند. فرض می‌کنیم که حالت واقع نیز حالت 1 باشد (یعنی روی نامه p نوشته شده باشد).

عملهای شناختی زیر ممکن است اتفاق بیفتد.

(۱) **بلند خواندن:** عامل a پاکت را باز می‌کند و نامه (گزاره p) را در حضور b بلند می‌خواند.

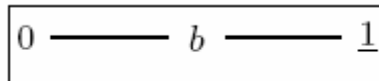
از آنجا که حالت واقع حالت ۱ است و نامه بلند خوانده شده است، گزاره p اعلان عمومی می‌شود. بعد از انجام این عمل شناختی، مدل کریپکی دانش بصورت زیر خواهد بود.

$$\boxed{1}$$

(دقت کنید که در مدل بالا (و همچنین مدل‌های دیگر) دو طوق با برچسب‌های a و b وجود دارد که برای جلوگیری از شلوغی شکل از کشیدن آنها صرف نظر شده است.)

(۲) **آهسته خواندن:** عامل a پاکت را باز می‌کند و نامه (گزاره p) را در حضور b آهسته می‌خواند.

عامل a از محتویات نامه آگاه می‌شود و گزاره p را می‌داند و عامل b تنها می‌داند که عامل a خبر داخل نامه را می‌داند اما خود از اینکه یا خبر p است یا $\neg p$ مطلع نیست. بعد از انجام این عمل شناختی، مدل کریپکی دانش بصورت زیر خواهد بود.



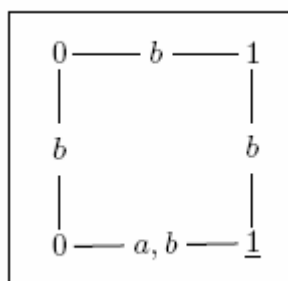
بعد از انجام این عمل، هنوز عامل b بین دو حالت ممکن سیستم (یعنی 0 و 1) مردد است در حالی که b می‌داند عامل a می‌داند که کدام حالت، حالت واقع است.

دقت کنید که یک اعلان خصوصی اتفاق افتاده است و در حالی که عامل a گزاره p را خوانده است، عامل b بین اینکه "عامل a گزاره p را خوانده است" یا "عامل a گزاره $\neg p$ را خوانده است" مردد است.

۳) شاید خواندن: عامل b برای چند دقیقه اتاق را ترک می‌کند و بر می‌گردد. در این فاصله a

نامه (گزاره p) را نمی‌خواند. عامل b این را ممکن می‌داند که شاید a نامه را در غیاب او خوانده باشد.

مدل کریپکی دانش بعد از انجام این عمل به صورت زیر خواهد بود.



در ادامه به این می‌پردازیم که مدل‌های کریپکی دانش بدست آمده بعد از انجام عملهای شناختی چگونه از روی مدل آغازین سیستم به دست می‌آیند.

۴-۴-۱ مدل کریپکی عمل شناختی

در بالا سه عمل شناختی را معرفی کردیم. در عمل شناختی "بلند خواندن" هر دو عامل دقیقاً می‌دانند که چه اتفاقی رخ داده است و آن اتفاق اعلان عمومی گزاره p است. اما در عمل دوم و سوم اینگونه نیست.

در عمل دوم، در حالی که عامل a می‌داند که دقیقاً چه اتفاقی افتاده است (اتفاق: a گزاره p را خوانده است)، عامل b بین اینکه "عامل a گزاره p را خوانده است" یا "عامل a گزاره $\neg p$ را خوانده است" مردد است.

در عمل سوم نیز، در حالی که عامل a می‌داند که دقیقاً چه اتفاقی افتاده است (اتفاق: a نامه را نخوانده است)، عامل b بین اینکه "عامل a گزاره p را خوانده است" یا "عامل a گزاره $\neg p$ را خوانده است" یا اینکه "عامل a نامه را باز نکرده و اتفاقی در مورد نامه نیفتاده است" مردد است.

در قبل به این نکته در مورد سیستم‌های چند عاملی اشاره کردیم که:

برای یک سیستم چند عاملی تعدادی حالت ممکن وجود دارد که یکی از آنها حالت واقع است، و هر

عامل با توجه به میزان دسترسی‌اش به اطلاعات بین تعدادی از حالت‌های ممکن نمی‌تواند تمیز قایل

شود.

اکنون نکته دیگری از سیستم‌های چند عاملی را مورد اشاره قرار می‌دهیم که:

در یک سیستم چند عاملی وقتی عملی اتفاق می‌افتد. هر عامل، با توجه به میزان دسترسی‌اش به

اطلاعات در مورد آن عمل، عمل واقع را نمی‌تواند با بعضی عمل‌های دیگر تمیز دهد.

تعریف ۴-۴-۱ یک مدل کریپکی عمل شناختی N برای یک سیستم چند عاملی با مجموعه عاملهای A و با مجموعه گزاره‌های اتمی P ، چند تایی

$$N = \langle S, (\sim_a)_{a \in A}, pre \rangle$$

است که

- S مجموعه همه حالت‌های ممکن برای عمل شناختی است،
- برای هر عامل $a \in A$ ، $\sim_a \subseteq S \times S$ رابطه‌ای $\sim_a$ بین حالت‌های عمل شناختی است که مشخص می‌کند عامل a با توجه به میزان دسترسی‌اش به اطلاعات سیستم، چه حالت‌هایی از عمل را نمی‌تواند از هم تمیز دهد، و
- تابع $pre : S \rightarrow L(P, A)$ یک تابع پیش‌شرط^{۵۰} است که به هر حالت ممکن یک فرمول در زبان $L(P, A)$ (که می‌تواند یک زبان مناسب در منطق شناختی باشد) به عنوان پیش‌شرط متناظر می‌کند.

برای هر $s \in S$ زوج (N, s) یک حالت واقع عمل نامیده می‌شود.

برای بهتر فهمیدن تعریف بالا، برای سه عمل شناختی بلند-خواندن، آهسته-خواندن و شاید-خواندن، به ترتیب مدل کریپکی عمل آنها را در زیر مشخص می‌کنیم.

- برای عمل بلند-خواندن تنها یک حالت ممکن برای هر دو عامل قابل تصور است. پس مجموعه

$$S = \{s\} \text{ فقط شامل}$$

⁵⁰ انتهای بخش ۳-۱-۳ را ببینید.

یک حالت است

s : عامل a گزاره p را می‌خواند

از طرفی هر دو عامل a و b بر این عمل آگاه هستند و داریم $s \sim_a s$ و $s \sim_b s$. پیش‌شرط s نیز گزاره p است، یعنی $pre(s) = p$.

• برای عمل آهسته-خواندن، از نگاه عامل b دو حالت ممکن است.

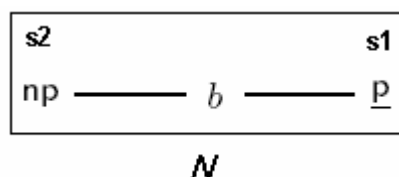
s_1 : عامل a گزاره p را می‌خواند

s_2 : عامل a گزاره $\neg p$ را می‌خواند

یعنی $S = \{s_1, s_2\}$. عامل a می‌تواند بین این دو حالت تمیز قایل شود ولی عامل b نمی‌تواند بین s_1 و s_2 تمیز دهد، پس $s_1 \sim_b s_2$. تابع پیش‌شرط نیز به صورت زیر خواهد بود

$$pre(s_1) = p, pre(s_2) = \neg p$$

تابع پیش‌شرط این را می‌گوید که مثلاً برای آنکه s_1 اتفاق بیفتد ("عامل a گزاره p را بخواند") باید روی نامه گزاره p نوشته شده باشد. شکل زیر مدل کریپکی عمل آهسته-خواندن است.



(np در شکل پیش‌شرط حالت s_2 است و همان $\neg p$ است که به این صورت نوشته شده است.)

حالت واقع عمل (N, s_1) است.

- برای عمل شاید-خواندن، از نگاه عامل b سه حالت ممکن است.

s_1 : عامل a گزاره p را می‌خواند

s_2 : عامل a گزاره $\neg p$ را می‌خواند

s_3 : عامل a نامه را نمی‌خواند

یعنی $S = \{s_1, s_2, s_3\}$. عامل a می‌تواند بین هر سه حالت تمیز قایل شود ولی عامل b نمی‌-

تواند بین این حالتها تمیز دهد، پس $s_1 \sim_b s_2$ ، $s_1 \sim_b s_3$ و $s_2 \sim_b s_3$. تابع پیش‌شرط نیز به

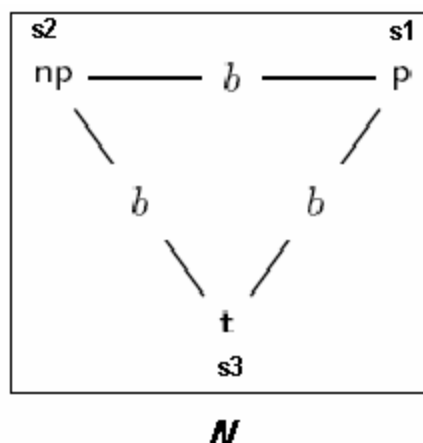
صورت زیر خواهد بود

$$pre(s_1) = p, pre(s_2) = \neg p, pre(s_3) = true$$

$pre(s_3) = true$ این معنا را می‌دهد که برای اینکه حالت s_3 اتفاق بیفتد هیچ پیش‌شرطی لازم

نیست.

شکل زیر مدل کریپکی عمل شاید-خواندن است.



حالت واقع عمل (N, s_3) است.

۴-۴-۲ به روز رسانی یک مدل دانش با یک مدل عمل

فرض کنید که M یک مدل کریپکی دانش و N یک مدل عمل شناختی برای یک سیستم چند عاملی با عاملهای A و مجموعه اتمی P باشد. فرض کنید حالت واقع سیستم (M, t) و حالت واقع عمل (N, s) باشد. می‌خواهیم تعریف کنیم که چگونه (M, t) با انجام عمل (N, s) به روز رسانی شده و مدل نقطه‌ای جدید (M', t') بدست می‌آید.

به عنوان نمونه، مثال دو دوست a و b ، و نامه روی میز را در نظر بگیرید. برای سیستم، دو حالت با توجه به محتویات نامه که p باشد یا $\neg p$ ممکن است. که حالت واقع سیستم را حالتی فرض کردیم که نامه خبر p را داشته باشد. برای عمل شاید-خواندن نیز از بین سه حالت ممکن، حالت واقع حالتی است که a نامه را نمی‌خواند. حال بعد از اینکه عامل b به اتاق برمی‌گردد مدل کریپکی دانش به چه صورت است؟

تعریف ۴-۴-۲ (به روز رسانی). فرض کنید برای مدل کریپکی دانش $M = \langle S_M, \pi, (R_a)_{a \in A} \rangle$ ، مدل نقطه‌ای (M, t) حالت واقع یک سیستم چند عاملی باشد و برای مدل عمل شناختی $N = \langle S_N, (\sim_a)_{a \in A}, pre \rangle$ عمل واقع (N, s) باشد. به روز رسانی (M, t) با عمل (N, s) مدل نقطه‌ای (M', t') است، که به صورت زیر تعریف می‌شود.

$$M' = \langle S_{M'}, \pi', (R'_a)_{a \in A} \rangle$$

$$S_{M'} = \{(v, w) \in S_M \times S_N \mid (M, v) \models pre(w)\} \quad \bullet$$

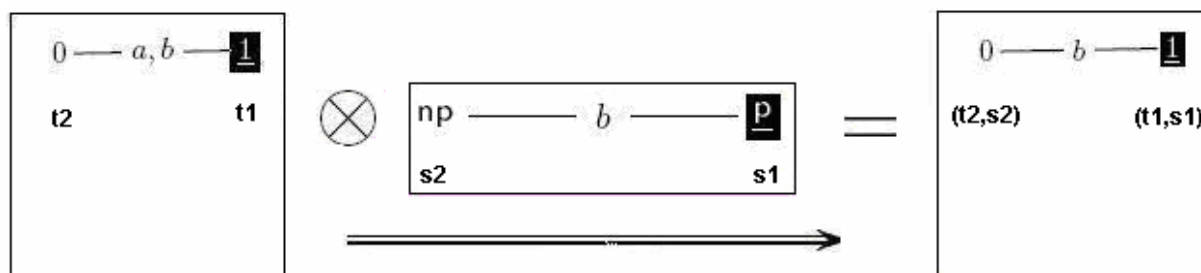
$$\pi'(v, w) = \pi(v), (v, w) \in S_{M'} \quad \bullet$$

• برای هر $a \in A$ ، $(v, w), (v', w') \in R'_a$ iff $(v, v') \in R_a$ and $(w, w') \in \sim_a$

حالت واقع بعد از به روز رسانی (M', t') است که $t' = (s, t)$.

برای نمونه به روز رسانی‌های عمل‌های شناختی آهسته-خواندن و شاید-خواندن روی مدل کریپکی آغازین بصورت زیر است.

به روز رسانی آهسته-خواندن:



مدل به روز رسانی شده M' شامل دو حالت ممکن است، $S_{M'} = \{(t_1, s_1), (t_2, s_2)\}$. دقت کنید که

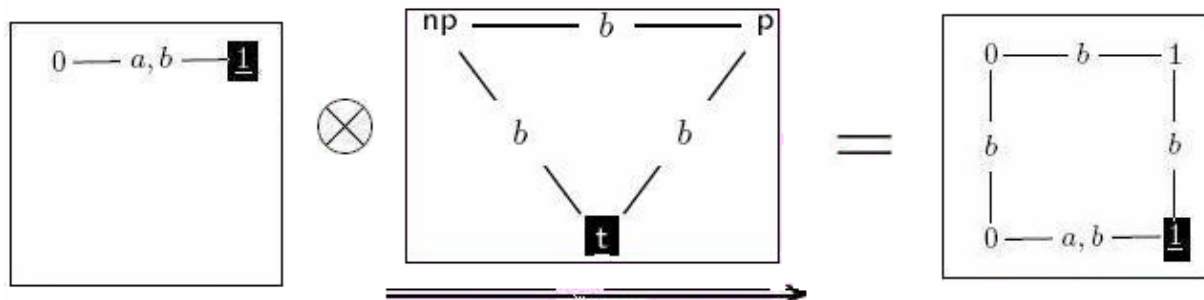
زوج‌مرتبه‌های (t_1, s_2) و (t_2, s_1) نمی‌تواند حالت‌های ممکن مدل M' باشند زیرا $pre(s_2) = \neg p$ است و

$(M, t_1) \not\models \neg p$ ، همچنین $pre(s_1) = p$ است و $(M, t_2) \not\models p$.

از آنجا که $(t_1, t_2) \in R_b$ و $(s_1, s_2) \in \sim_b$ داریم $((t_1, s_1), (t_2, s_2)) \in R'_b$.

به روز رسانی شاید-خواندن:

شکل زیر نیز به روز رسانی شاید-خواندن را نمایش می‌دهد.



تمرین. دو دوست a, b اتاق نشیمن را ترک و نامه روی میز بدون خواندن رها می کنند. عامل a به آشپزخانه و عامل b به اتاق خواب می رود. این امکان وجود دارد که هر کدام آنها یواشکی سری به اتاق نشیمن بزنند. بعد از چند هر دو با هم به اتاق نشیمن بر می گردند آگاهی آنها چگونه تغییر کرده است؟ عمل شناختی متناظر را معرفی کنید؟ مدل کریپکی به روزسانی شده با عمل فوق را رسم کنید.

۴-۵ مدل سازی

در این فصل، به کاربرد منطق شناختی در مدل کردن پروتکلها و خواص امنیت می پردازیم. ابتدا دو

مطالعه موردی (۱) محرمانگی با اعلان عمومی و (۲) توصیف گمنامی، را بررسی می کنیم.

سپس به این خواهیم پرداخت که در روش صوری^{۵۲} منطق شناختی چگونه ...

○ ... یک پروتکل را به کمک یک دنباله از عملهای شناختی شرح^{۵۳} دهیم،

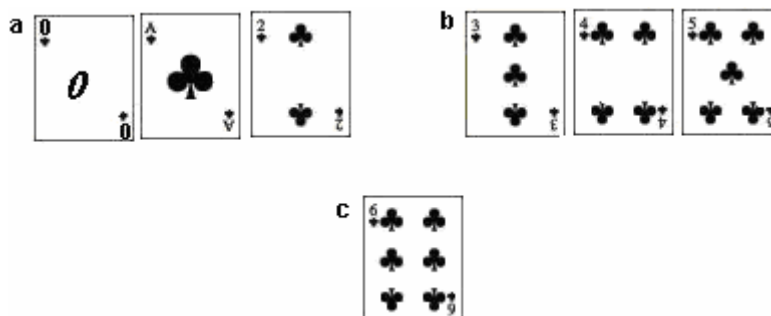
○ ... یک خاصیت امنیت را به کمک یک فرمول در منطق شناختی توصیف^{۵۴} کنیم،

○ ... خاصیت امنیت را برای پروتکل درستیابی^{۵۵} کنیم.

۴-۵-۱ محرمانگی با اعلان عمومی

در مباحث امنیت، عموماً فرض بر این است که کانالهای ارتباطی امن نیستند و اگر دو عامل بخواهند خبری را با یکدیگر در میان بگذارند، شنود خبر برای عامل‌های دیگر ممکن است. به عبارتی دیگر، ارتباط از نوع اعلان عمومی است. در این بخش، مساله کارتهای روسی^{۵۶} را به عنوان مطالعه‌ای موردی در رمزنگاری با اعلان عمومی مورد بررسی قرار می‌دهیم.

یک دسته ۷ تایی کارت که روی آنها اعداد 0,1,2,3,4,5,6 نوشته شده است بین سه عامل a ، b و c توزیع شده است، به طوریکه به دو عامل a و b هر نفر سه کارت، و به عامل c یک کارت داده شده است.



عامل‌های a و b می‌خواهند همدیگر را از کارتهای خود مطلع کند بدون آنکه عامل c اطلاعی در مورد دست آنها پیدا کند. اما سیستم ارتباطی به گونه‌ای است که هر خبری را که یکی از عاملها برای عاملی دیگر می‌فرستد، همه عاملها از آن مطلع می‌شوند. یعنی ارتباط دو عامل تنها از راه اعلان عمومی میسر است.

به شناسایی و درستیابی پروتکل‌های ارتباطی اعلان عمومی برای تبادل اطلاعات دو عامل a و b ، به طوریکه عامل c هیچ اطلاعی در مورد توزیع کارتها پیدا نکند، خواهیم پرداخت.

مساله کارتهای روسی از دو قسمت تشکیل می‌شود ۱. سیستم چند عاملی آن ۲. پروتکلی که شرایط نهایی مساله را برآورده می‌سازد. در منطق شناختی، سیستم چند عاملی با مشخص شدن مجموعه گزاره‌های اتمی و مدل کریپکی مشخص می‌شود، و پروتکل با یک دنباله متناهی از عمل‌های شناختی (یا اعلانهای عمومی) بیان می‌گردد. برای آنکه پروتکل شرایط نهایی مساله را برآورده کند باید مدل کریپکی به روز رسانی شده توسط عملهای داخل پروتکل، شرایط نهایی را ارضا کند.

۴-۵-۱-۱ سیستم چند عاملی کارتهای روسی

برای آنکه سیستم چند عاملی مساله کارتهای روسی را مدل کنیم ابتدا باید دو مجموعه A (مجموعه عاملها) و P (مجموعه گزاره‌های اتمی سیستم) را مشخص کنیم. مجموعه عالمها $A = \{a, b, c\}$ است. مجموعه گزاره‌های اتمی

$$P = \{i_e \mid 0 \leq i \leq 6 \ \& \ e \in \{a, b, c\}\}$$

که گزاره i_e یعنی کارت i در دست عامل e است. برای سادگی از اختصار زیر در ادامه بخش استفاده می‌کنیم.

$$ijk_e \equiv i_e \wedge j_e \wedge k_e, \quad 0 \leq i < j < k \leq 6, e \in \{a, b\}$$

ijk_e دست عامل $e \in \{a, b\}$ را نشان می‌دهد که از سه کارت متمایز تشکیل می‌شود.

اکنون با داشتن گزاره‌های اتمی سیستم می‌توانیم شرایط نهایی^{۵۷} مساله کارتهای روسی را که باید بعد از انجام یک پروتکل بدست آید را به کمک گزاره‌های منطق شناختی توصیف^{۵۸} کنیم.

سه گزاره زیر را در نظر بگیرید.

۱. عامل a کارتهای عامل b را بداند. این جمله را با گزاره زیر در منطق شناختی توصیف می‌کنیم.

$$a\text{-knows-}b\text{'s}: \bigwedge_{0 \leq i < j < k \leq 6} (ijk_b \rightarrow K_a(ijk_b))$$

۲. عامل b کارتهای عامل a را بداند. این جمله را با گزاره زیر در منطق شناختی توصیف می‌کنیم.

$$b\text{-knows-}a\text{'s}: \bigwedge_{0 \leq i < j < k \leq 6} (ijk_a \rightarrow K_b(ijk_a))$$

۳. عامل c هیچ اطلاعی در مورد کارتهای عامل‌های a و b را ندارد. این جمله را با گزاره زیر در منطق شناختی توصیف می‌کنیم.

$$c\text{-ignorant}: \bigwedge_{0 \leq i \leq 6} (\neg K_c(i_a) \wedge \neg K_c(i_b))$$

شرایط نهایی مورد نظر مساله کارتهای روسی به صورت زیر توصیف می‌شوند.

• $C_{ab}(a\text{-knows-}b\text{'s} \wedge b\text{-knows-}a\text{'s})$. بعد از اجرای پروتکل باید عامل‌های a و b

کارتهای یکدیگر را بدانند و این دانستن بین آنها یک همه‌دانی مشترک^{۵۹} باشد

⁵⁷ Post conditions

⁵⁸ Specify

⁵⁹ Common knowledge

• $C_{abc}(\text{c-ignorant})$. همه عاملهای a, b, c همه‌دانی مشترک در مورد این موضوع داشته

باشند که عامل c هیچ اطلاعی در مورد کارتهای دو عامل دیگر بعد از اجرای پروتکل

بدست نمی‌آورد.

بعد از مشخص کردن فرمولهای اتمی سیستم، باید مدل کریپکی دانش سیستم را مشخص کرد. هر

حالت سیستم یک نوع توزیع کارت بین عاملها است. از آنجا که باید به عاملهای a و b هر کدام سه

کارت و به عامل c یک کارت بدهیم تعداد حالتهای ممکن عبارت است از

$$\binom{7}{3} \binom{4}{3} = 140$$

هر حالت را به شکل

$$ijk \mid lmn \mid t$$

که $i < j < k, l < m < n$ و $\{i, j, k, l, m, n, t\} = \{0, 1, 2, 3, 4, 5, 6\}$ است، نمایش می‌دهیم.

یعنی فضای حالتهای سیستم عبارت است از

$$S = \left\{ ijk \mid lmn \mid t \mid i < j < k, l < m < n, \{i, j, k, l, m, n, t\} = \{0, 1, 2, 3, 4, 5, 6\} \right\}$$

حالتی از سیستم است که کارتهای ijk در دست عامل a ، کارتهای lmn در دست

عامل b و کارت t در دست عامل c باشد. برای مثال $012 \mid 345 \mid 6$ یعنی عامل a کارتهای $0, 1, 2$ ،

عامل b کارتهای $3, 4, 5$ و عامل c کارت 6 را دارد.

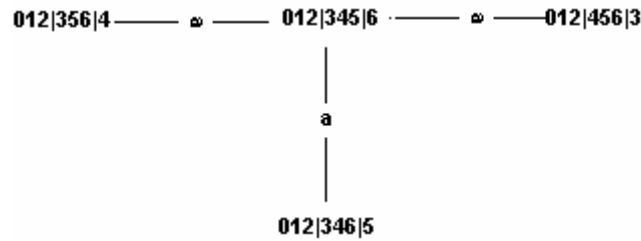
تابع ارزشدهی $\pi : S \rightarrow 2^P$ به صورت زیر تعریف می‌شود

$$\pi(ijk | lmn | t) = \{i_a, j_a, k_a, l_b, m_b, n_b, t_c\}$$

هر عامل با توجه به میزان دسترسی‌اش به اطلاعات سیستم بین بعضی از حالات مردد است. توجه کنید که هر عاملی که کارت بیشتری در دست دارد میزان دسترسی‌اش به اطلاعات سیستم بیشتر است.

عامل a تنها دست خود را می‌بیند. به این ترتیب او نمی‌تواند حالت $ijk | lmn | t$ را از حالتی که چهار کارت l, m, n, t به ترتیب‌های بین دو عامل به دلخواه دیگر توزیع شوند تمیز دهد. این چهار کارت به $\binom{4}{3}$ روش می‌تواند بین دو نفر دیگر توزیع شود. برای مثال عامل a نمی‌تواند حالت $012 | 345 | 6$ را از حالتی

$012 | 346 | 5$ ، $012 | 356 | 4$ ، $012 | 456 | 3$ تمیز دهد.



به همین ترتیب، عامل b نیز نمی‌تواند هر حالت را از ۴ حالت دیگر تمیز دهد. عامل c نیز تنها دست خود را که شامل یک کارت است می‌بیند. شش کارت دیگر می‌تواند به $\binom{6}{3}$ روش بین دو عامل دیگر توزیع شود. پس برای عامل c ، هر حالت سیستم از ۲۰ حالت قابل تمیز نیست.

$$(ijk | lmn | t, i'j'k' | l'm'n' | t') \in R_a \Leftrightarrow i = i' \ \& \ j = j' \ \& \ k = k'$$

$$(ijk | lmn | t, i'j'k' | l'm'n' | t') \in R_b \Leftrightarrow l = l' \ \& \ m = m' \ \& \ n = n'$$

$$(ijk \mid lmn \mid t, i'j'k' \mid l'm'n' \mid t') \in R_c \Leftrightarrow t = t'$$

به این ترتیب گراف دانش (مدل کریپکی) مساله کارتهای روسی از ۱۴۰ گره تشکیل می‌شود که از هر گره

▪ ۴ یال با برچسب a (دقت کنید که یکی از این یالها طوق است)،

▪ ۴ یال با برچسب b (یکی از این یالها طوق است)،

▪ و ۲۰ یال با برچسب c (یکی از این یالها طوق است)،

خارج می‌شود.^{۶۰}

با فراهم بودن مجموعه گزاره‌های اتمی و مدل کریپکی مساله کارتهای روسی، این سیستم چند عاملی به طور کامل به روش صوری منطق شناختی بیان شده است.

۴-۵-۱-۲ پروتکل‌های مساله کارتهای روسی

به یک پروتکل برای مساله کارتهای روسی، **پروتکل مستقیم** گوییم، هرگاه پروتکل از دو مرحله، که به ترتیب توسط عامل‌های a و b انجام می‌شوند، تشکیل شود. به این ترتیب که، عامل a گزاره‌ای، چون φ ، را (با توجه به میزان دسترسی‌اش به اطلاعات) بلند بیان می‌کند سپس عامل b گزاره‌ای، چون ψ ، را (با توجه به میزان دسترسی‌اش به اطلاعات) بیان می‌کند و شرایط نهایی مساله^{۶۱} حاصل می‌شود. در این بخش به بررسی پروتکل‌های مستقیم مساله خواهیم پرداخت.

همانطور که گفتیم پروتکل مستقیم شامل دو مرحله است:

⁶⁰ از آنجا که تعداد گره‌ها و یالهای گراف زیاد است، گراف را رسم نمی‌کنیم.

⁶¹ Post conditions

(۱) عامل a گزاره‌ای، چون φ ، را بلند بیان می‌کند،

(۲) عامل b گزاره‌ای، چون ψ ، را بلند بیان می‌کند.

بگذارید مشخص کنیم وقتی که عامل a گزاره صادق φ را بلند بیان می‌کند، چه گزاره‌ای اعلان

عمومی می‌شود؟ در نگاه اول، ممکن است پاسخ این باشد که گزاره‌ای که اعلان عمومی شده است

همان φ است، اما در واقع چیز بیشتری اعلان عمومی می‌شود. به دو نکته باید در اینجا توجه کرد:

اول اینکه: عامل a گزاره φ را بلند بیان می‌کند تا به این ترتیب، با این اطلاع جدید، عامل b از

کارتهای عامل a مطلع شود. عامل a گزاره φ را با توجه به کارتهای دست خود می‌سازد، پس a

گزاره φ را باید بداند. بنابراین، وقتی a گزاره φ را بلند بیان می‌کند گزاره $K_a\varphi$ نیز اعلان عمومی

می‌شود.

دوم اینکه: در یک پروتکل صحیح، وقتی عامل a گزاره φ را بلند بیان می‌کند متوجه این موضوع

هست که عامل c نباید هیچ اطلاعی در مورد کارتهای a, b پیدا کند و عاملهای دیگر از این که او

متوجه این موضوع هست آگاهند. عامل a ، بدون آنکه چیزی بگوید، این اطمینان را دارد می‌دهد که

بلند گفتن φ ، سبب لو رفتن کارتها نمی‌شود. بنابراین، وقتی a گزاره φ را بلند بیان می‌کند گزاره

$C_{abc}(\text{c-ignorant})$ نیز اعلان عمومی می‌شود.

به این ترتیب، اینکه عامل a گزاره φ را بلند بیان کند معادل است با دو اعلان عمومی متوالی

$$[K_a\varphi][C_{abc}(\text{c-ignorant})]$$

یعنی وقتی عامل a گزاره φ را بلند می‌گوید این اعلان عمومی صورت می‌گیرد که

"عامل a ، گزاره φ را می‌داند و پس از اعلان این دانستن (از آنجا که a متوجه است که نباید c

اطلاعی پیدا کند) هنوز عامل c هیچ اطلاعی در مورد کارتهای دو عامل دیگر ندارد"

همینطور، اینکه عامل b گزاره ψ را بلند بیان کند معادل است با دو اعلان عمومی

$$.[K_b\psi][C_{abc}(\text{c-ignorant})]^{62}$$

پس یک پروتکل مستقیم عبارت از چهار اعلان عمومی متوالی بصورت زیر است:

$$.[K_a\varphi][C_{abc}(\text{c-ignorant})][K_b\psi][C_{abc}(\text{c-ignorant})]$$

به یک پروتکل مستقیم موفق گوییم، هرگاه مدل حاصل از به روز رسانی مدل آغازین به کمک پروتکل، شرایط نهایی مساله را ارضا کند. در غیر اینصورت، پروتکل را ناموفق می‌نامیم.

یک پروتکل مستقیم ناموفق

فرض می‌کنیم حالت واقع $t \mid ijk \mid lmn$ باشد. عامل a تنها دست خود (یعنی کارتهای i, j, k) را می‌بیند و از دست دیگران مطلع نیست.

- پروتکل ناموفق: عامل a می‌گوید

"یا هر سه کارت i, j, k در دست من است یا هیچکدام از آنها در دست من نیست."

⁶² یک مساله مهم در بررسی یک پروتکل درست شرح دادن (description) و درست توصیف کردن (specification) آن است. اگر در مرحله‌ای که یک سیستم چند عاملی یا یک پروتکل را به روش صوری منطق شناختی شرح می‌دهیم دچار اشتباه شویم (مثلا عمل‌ها را اشتباه بیان کنیم یا شرایط نهایی را با گزاره‌هایی نامناسب متناظر کنیم) آنگاه آنچه را که درست‌یابی (حتی اگر درست‌یابی (verification) را دقیق انجام دهیم) می‌کنیم با واقعیت متمایز خواهد بود.

گزاره $\varphi = ijk_a \vee \neg(i_a \vee j_a \vee k_a)$ گزاره‌ای است که عامل a آن را بلند می‌گوید این بلند

گفتن معادل است با اینکه اعلان عمومی

$$[K_a(ijk_a \vee \neg(i_a \vee j_a \vee k_a))][C_{abc}(\text{c-ignorant})]$$

اتفاق افتد. پروتکل ناموفق است.

عامل c اینگونه استدلال می‌کند:

وقتی عامل a می‌گوید "یا هر سه کارت i, j, k در دست من است یا هیچکدام از آنها در دست من نیست" و متوجه این موضوع است که من نباید هیچ اطلاعی در مورد کارتها پیدا کنم و در مورد این موضوع دارد (به خود و عامل b) اطمینان می‌دهد، پس باید هر سه کارت i, j, k در دست خودش باشد. زیرا در غیر اینصورت، او نمی‌تواند در مورد اینکه من هیچ اطلاعی پیدا نمی‌کنم اطمینان داشته باشد. چون اگر هیچ یک از کارتهای i, j, k در دست a نباشد، عامل a این امکان را می‌دهد که یکی از سه کارت i, j, k در دست من باشد و من با شنیدن "یا هر سه کارت i, j, k در دست a است یا هیچکدام از آنها در دست او نیست" و داشتن یکی از سه کارت، خواهم دانست که دو کارت دیگر در دست عامل b است.

در واقع بعد از آنکه مدل آغازین مساله کارتهای روسی را با عمل

$$[K_a(ijk_a \vee \neg(i_a \vee j_a \vee k_a))][C_{abc}(\text{c-ignorant})]$$

$C_{abc}(\text{c-ignorant})$ ارضا نمی‌شود.^{۶۳} اگر مدل آغازین مساله را (که شامل ۱۴۰ حالت ممکن است) با

Russian نشان دهیم، داریم

⁶³ بخش ۳-۳ به روز رسانی با اعلان عمومی را ببینید.

$$(\text{Russian}, ijk \mid lmn \mid t) \models [K_a(ijk_a \vee \neg(i_a \vee j_a \vee k_a))][C_{abc}(\text{c-ignorant})] \neg C_{abc}(\text{c-ignorant})$$

یک پروتکل مستقیم موفق

فرض می‌کنیم حالت واقع $ijk \mid lmn \mid t$ باشد.

• پروتکل موفق:

(a) عامل a می‌گوید "دست من یکی از دسته کارتهای ijk, ilm, int, jln, kmt است."

عامل a پنج دسته کارت سه تایی را که در شرایط زیر صدق می‌کنند، برای اعلان عمومی اینکه

دست او یکی از این پنج دسته است انتخاب می‌کند. بگذارید H مجموعه این ۵ دسته و h_a

دست عامل a باشد

۱. $P_1(h_a)$ یکی از پنج دسته، دست خود او باشد

$$P_1(h) \equiv h \in H$$

۲. برای هر دسته چون h ، در هر یک از چهار دسته دیگر، حداقل ۲ کارت باشد که در

دسته h نیست $\forall h \in H P_2(h)$

$$P_2(h) \equiv (\forall h' \in H - h)(\exists x, z)(x \in h' \wedge z \in h' \wedge x \notin h \wedge z \notin h)$$

۳. برای هر کارت z ، اگر دسته‌هایی که شامل z هستند را حذف کنیم، هر کارت دیگر به غیر از z ، حداقل متعلق به یکی از دسته‌های باقی مانده باشد ولی متعلق به همه دسته‌های باقی مانده نباشد

$$P_3 \equiv \forall (z \rightarrow (\forall (x \neq z \rightarrow (\exists h \in \{h' \in H \mid z \notin h'\} \mid x \in h \wedge \exists h' \in \{h' \in H \mid z \notin h'\} \mid x \notin h))))))$$

(b) سپس عامل b می‌گوید "کارت t در دست عامل c است."

عامل a تنها دست خود را می‌بیند. او می‌داند که باید گزاره‌ای، چون

$$\varphi = ijk_a \vee ilm_a \vee int_a \vee jln_a \vee kmt_a$$

را در مورد دستش بلند بگوید بطوریکه عامل b با توجه به میزان دسترسی‌اش به اطلاعات، دست a را بفهمد، اما عامل c که میزان دسترسی‌اش به اطلاعات کل سیستم از b کمتر است، هیچ اطلاعی پیدا نکند. به این منظور، عامل a پنج دسته کارت را اعلان می‌کند، که یکی از این دسته کارت‌ها (دسته ijk) دست واقعی او است. در هر دسته کارت دیگر، عامل a یک کارت از کارت‌های خودش و دو کارت از کارت‌هایی که در دستش نیست را در نظر می‌گیرد. عامل b حداقل یکی از دو کارت دیگر را دارد پس می‌تواند متوجه شود از بین ۵ دسته کدام دسته، دست عامل a است.

عامل b کارت‌های l, m, n را دارد و نتیجه می‌گیرد که ۴ دسته ilm, int, jln, kmt که شامل حداقل یک کارت از کارت‌های او است را باید خط بزند. از آنجا که a گفته است که دست او یکی از این ۵ دسته است، عامل b می‌فهمد که ijk دست a است.

عامل a اطمینان دارد که بعد از بلند گفتن φ عامل c هیچ اطلاعاتی در مورد کارتهای دو عامل a, b پیدا نمی‌کند. عامل a اینگونه استدلال می‌کند که یکی از چهار کارت l, m, n, t در دست c است.

❖ اگر l در دست c باشد آنگاه عامل c فقط می‌تواند دو دسته ilm, jln را خط بزند و سه دسته ijk, int, kmt باقی می‌ماند. در بین سه دسته باقی مانده، برای هر کارتی چون v به جز l ، حداقل یک دسته هست که شامل v است و یک دسته هست که شامل v نیست. پس c هیچ اطلاعاتی در حالتی که کارت l در دست او باشد نمی‌تواند در مورد آنکه v کارت دست کیست بدست آورد.

❖ اگر m در دست c باشد آنگاه عامل c فقط می‌تواند دو دسته ilm, kmt را خط بزند و سه دسته ijk, int, jln باقی می‌ماند. هر یک از کارتهای i, j, k, l, n حداقل در یکی از این دسته‌ها قرار دارند. همچنین برای هر کارت i, j, k, l, n ، حداقل یکی از این سه دست هست که شامل آن نیست. پس c هیچ اطلاعاتی در حالتی که کارت m در دست او باشد نمی‌تواند بدست آورد.

❖ به همین ترتیب می‌توان بررسی کرد که عامل c نمی‌تواند در حالتی که کارتهای n, t در دست او باشد نیز اطلاعاتی در این مورد که چه کارتی در دست چه کسی است بدست آورد.

مسئله ما نیازی به استدلال‌های بالا نداریم و روشی اتوماتیک برای درست‌یابی پروتکل داریم. به این

ترتیب که مدل آغازین مساله Russian را با اعلان‌های عمومی زیر

$$[K_a\varphi][C_{abc}(\text{c-ignorant})]$$

$$[K_b\psi][C_{abc}(\text{c-ignorant})]$$

در دو مرحله به روز رسانی می‌کنیم. در مرحله اول (به روز رسانی با $[K_a\varphi][C_{abc}(\text{c-ignorant})]$) بررسی می‌کنیم که آیا مدل حاصل، Russian_1 ، گزاره $C_{abc}(\text{c-ignorant})$ را ارضا می‌کند. سپس مدل Russian_1 را با $[K_b\psi][C_{abc}(\text{c-ignorant})]$ به روز رسانی می‌کنیم. بررسی می‌کنیم که آیا در مدل حاصل، Russian_2 ، شرایط نهایی $C_{ab}(\text{a-knows-b's} \wedge \text{b-knows-a's})$ و $C_{abc}(\text{c-ignorant})$ ارضا می‌شود.

از آنجا که تعداد حالت‌های مدل ۱۴۰ است. انجام دادن به روز رسانی به صورت دستی کاری زمان‌بر است برای این منظور ابزارهایی برای چک کردن مدل‌ها^{۶۴} چون $\text{MCK}^{۶۵}$ ([9]) و $\text{DEMO}^{۶۶}$ ([9]) فراهم شده است.

برای مطالعه بیشتر در مورد مساله کارتهای روسی مراجع [6,8,9] را ببینید.

۴-۵-۲ گمنامی

گمنامی^{۶۷} به عنوان یک مفهوم امنیت هدف بسیاری از پروتکل‌های سیستم‌های چند عاملی چون رای-گیری الکترونیکی، حراجی‌ها، تسهیم کردن^{۶۸}، و . . . می‌باشد. در این بخش مساله میز شام رمزنگاران^{۶۹} [11] را به کمک منطق شناختی توصیف و درستیابی می‌کنیم.

سه رمزنگار a, b, c دور یک میزگرد شام می‌خورند. بعد از شام متوجه می‌شوند که صورت حساب پرداخته شده است. در مورد این موضوع که یا یکی از رمزنگارها صورت حساب را پرداخته است یا سازمان امنیت کشور توافق (همه‌دانی مشترک) وجود دارد.

رمزنگارها می‌خواهند بدانند که آیا یکی از آنها پرداخت کننده بوده است یا سازمان امنیت. اما آنها می‌خواهند در صورتی که یکی از آنها پرداخت کننده باشد هویت او لو نرود و گمنام باقی بماند.

به این منظور پروتکل زیر را اجرا می‌کنند:

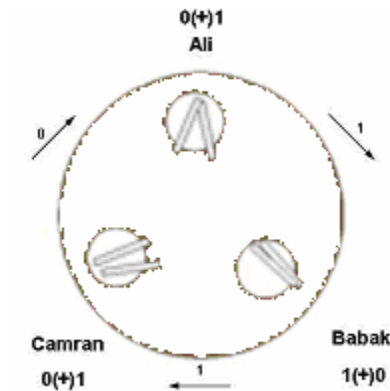
هر رمزنگار یک رقم 0 یا 1 را به دلخواه برای خود انتخاب می‌کند. سپس به طور خصوصی رقم خود را به نفر سمت چپ خود اعلان می‌کند. هر رمزنگار رقم دریافتی را (رقمی را که از نفر سمت راستی خود دریافت کرده است) با رقم انتخابی خود (رقمی که انتخاب کرده و به نفر سمت چپی خود فرستاده است) فصل ضمنی (XOR) می‌کند. اگر پرداخت کننده نباشد حاصل را به طور عمومی اعلان می‌کند وگرنه حاصل را با 1 جمع دودویی می‌کند و حاصل جمع جدید را به طور عمومی اعلان می‌کند. سه رقمی که اعلان عمومی شده است با هم جمع دودویی می‌شوند. اگر حاصل 0 باشد یعنی سازمان امنیت پرداخت کننده است، و اگر 1 باشد یعنی یکی از عاملها پرداخت کننده است.

Anonymity⁶⁷

Sharing⁶⁸

Dining Cryptographers Problem⁶⁹

(شکل زیر حالتی را نشان می‌دهد که هیچ یک از رمزنگارها پرداخت کننده نبوده است و سازمان امنیت پرداخت کرده است)



۴-۵-۲-۱ سیستم چند عاملی مساله

سیستم چند عاملی مساله میز شام رمزنگارها از سه عامل a, b, c تشکیل می‌شود و گزاره‌های اتمی سیستم عبارتند از

$$P = \{q_i, p_i \mid i \in \{a, b, c\}\}$$

که

p_i یعنی: "عامل i پرداخت کننده است".

q_i یعنی: "عامل i رقم 1 را انتخاب کرده است".

شرایط نهایی مساله (که باید بعد از انجام پروتکل بدست آید) با گزاره‌های زیر در منطق شناختی توصیف می‌شوند

(۱) گمنامی

$$[p_a \rightarrow C_{abc}(\neg K_b p_a \wedge \neg K_c p_a)] \wedge [p_b \rightarrow C_{abc}(\neg K_a p_b \wedge \neg K_c p_b)] \wedge [p_c \rightarrow C_{abc}(\neg K_b p_c \wedge \neg K_a p_c)]$$

(۲) یا همه عامل‌ها با هم بطور مشترک بدانند که پرداخت کننده سازمان امنیت است یا همه عامل‌ها با هم بطور مشترک بدانند که پرداخت کننده یک از آنها است.

$$C_{abc}(p_a \vee p_b \vee p_c) \vee C_{abc}(\neg p_a \wedge \neg p_b \wedge \neg p_c)$$

بعد از مشخص کردن فرمولهای اتمی سیستم، باید مدل کریپکی دانش سیستم را مشخص کرد. بگذارید تعداد حالت‌های ممکن سیستم را مشخص کنیم. ۴ حالت پرداخت ممکن است: ۱- عامل a پرداخت کند، ۲- عامل b پرداخت کند، ۳- عامل c پرداخت کند، و ۴- هیچ‌یک از عامل‌ها پرداخت نکنند (پرداخت کننده سازمان امنیت باشد^{۷۰}). هر عامل می‌تواند به دو طریق یک رقم ۰ یا ۱ را انتخاب کند. به این ترتیب تعداد کل حالت‌های سیستم عبارت است از

$$32 = 4 \times 2 \times 2 \times 2$$

مجموعه S می‌تواند به عنوان مجموعه حالت‌های سیستم در نظر گرفته شود.

$$S = \{ (x_a, x_b, x_c, y_a, y_b, y_c) \mid (\forall i \in \{a, b, c\})(x_i, y_i \in \{0, 1\}) \& \forall i, j \in \{a, b, c\}(x_i x_j = 0) \}$$

هر حالت یک ۶ تایی مرتب از رقم‌های ۰ و ۱ است به طوریکه حداکثر یکی از x_1, x_2, x_3 مخالف صفر است. هر x_i اگر ۱ باشد یعنی عامل i در این حالت پرداخت کننده است. مقدار y_i رقمی است که

⁷⁰ دقت کنید که سازمان امنیت را به عنوان یک عامل در سیستم چند عاملی خود در نظر نگرفتیم.

عامل i انتخاب کرده است تا برای نفر سمت چپی خود بفرستد. برای مثال $(0,1,0,1,1,1)$ حالتی از سیستم است که عامل b پرداخت کننده است و هر عامل می‌خواهد رقم 1 را به سمت چپی خود بفرستد.

تابع ارزشدهی $\pi : S \rightarrow 2^P$ بصورت زیر است: برای هر $i \in \{a, b, c\}$

$$p_i \in \pi((x_a, x_b, x_c, y_a, y_b, y_c)) \Leftrightarrow x_i = 1$$

$$q_i \in \pi((x_a, x_b, x_c, y_a, y_b, y_c)) \Leftrightarrow y_i = 1$$

هر عامل می‌داند که آیا پرداخت کننده است یا نه. همچنین، هر عامل از رقمی که می‌خواهد برای سمت چپی خود بفرستد مطلع است. به این ترتیب، روابط مدل کریپکی به صورت زیر است.

$$((x_a, x_b, x_c, y_a, y_b, y_c), (x'_a, x'_b, x'_c, y'_a, y'_b, y'_c)) \in R_a \Leftrightarrow x_a = x'_a \ \& \ y_a = y'_a$$

$$((x_a, x_b, x_c, y_a, y_b, y_c), (x'_a, x'_b, x'_c, y'_a, y'_b, y'_c)) \in R_b \Leftrightarrow x_b = x'_b \ \& \ y_b = y'_b$$

$$((x_a, x_b, x_c, y_a, y_b, y_c), (x'_a, x'_b, x'_c, y'_a, y'_b, y'_c)) \in R_c \Leftrightarrow x_c = x'_c \ \& \ y_c = y'_c$$

مدل کریپکی دانش مساله را با نماد Dining نشان می‌دهیم. در هر حالت ممکن گزاره‌های زیر ارضا می‌شوند.

- این یک همه‌دانی مشترک است که حداکثر یک نفر می‌تواند پرداخت کننده باشد.

$$(\text{Dining}, (x_a, x_b, x_c, y_a, y_b, y_c)) \models C_{abc}(\neg(p_a \wedge p_b) \wedge \neg(p_a \wedge p_c) \wedge \neg(p_b \wedge p_c))$$

- این یک همه‌دانی مشترک است که هر عاملی می‌داند که آیا پرداخت کننده هست یا نیست.

$$(\text{Dining}, (x_a, x_b, x_c, y_a, y_b, y_c)) \models C_{abc}((K_a p_a \vee K_a \neg p_a) \wedge (K_b p_b \vee K_b \neg p_b) \wedge (K_c p_c \vee K_c \neg p_c))$$

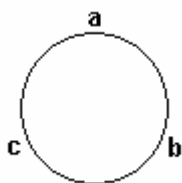
- این یک همه‌دانی مشترک است که هر عاملی از رقمی که به عامل دیگر فرستاده است مطلع است.

$$(\text{Dining}, (x_a, x_b, x_c, y_a, y_b, y_c)) \models C_{abc}((K_a q_a \vee K_a \neg q_a) \wedge (K_b q_b \vee K_b \neg q_b) \wedge (K_c q_c \vee K_c \neg q_c))$$

۴-۵-۲ پروتکل مساله

در پروتکل مساله میز شام رمزنگارها ابتدا سه اعلان خصوصی صورت می‌گیرد، به این ترتیب که هر عامل به عامل سمت چپی خود یک رقم دودویی می‌فرستد. سپس سه اعلان عمومی صورت می‌گیرد که هر عامل رقم خود را با رقمی که دریافت کرده است فصل XOR می‌کند. اگر پرداخت کننده نباشد حاصل را اعلان عمومی می‌کند وگرنه حاصل را با 1 جمع دودویی می‌کند و حاصل جمع جدید را اعلان عمومی می‌کند.

سه اعلان خصوصی را با عمل‌شناختی مدل می‌کنیم. فرض می‌کنیم عامل‌ها همانند شکل زیر دور میز نشسته‌اند:



همچنین فرض می‌کنیم $(x_a, x_b, x_c, y_a, y_b, y_c)$ حالت واقع باشد. اعلان‌های زیر در پروتکل اتفاق می‌افتد.

۱. عامل a رقم y_a را به طور خصوصی برای عامل b می‌فرستد.

عامل c نمی‌داند که آیا عامل a رقم 0 را فرستاده است یا رقم 1 را، و بین این دو موضوع مردد است. عمل شناختی زیر را برای مدل کردن این اعلان خصوصی در نظر می‌گیریم.

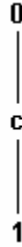
$$N_1 = \langle S_1, (\sim^1_i)_{i \in A}, pre_1 \rangle$$

$$S_1 = \{0, 1\} \quad \bullet$$

$$\sim^1_c = \{(0, 0), (1, 1), (0, 1), (1, 0)\} \text{ و } \sim^1_b = \sim^1_a = \{(0, 0), (1, 1)\} \quad \bullet$$

$$pre_1(1) = q_a \text{ و } pre_1(0) = \neg q_a \quad \bullet$$

عمل واقع (N_1, y_a) است. (شکل زیر مدل عمل N_1 را نشان می‌دهد که در آنها طوق‌ها را رسم نکرده‌ایم.)



۲. عامل b رقم y_b را به طور خصوصی برای عامل c می‌فرستد.

عامل a نمی‌داند که آیا عامل b رقم 0 را فرستاده است یا رقم 1 را، و بین این دو موضوع مردد است. عمل شناختی زیر را برای مدل کردن این اعلان خصوصی در نظر می‌گیریم.

$$N_2 = \langle S_2, (\sim^2_i)_{i \in A}, pre_2 \rangle$$

- $S_2 = \{0,1\}$

- $\sim_a^2 = \{(0,0), (1,1), (0,1), (1,0)\}$ و $\sim_b^2 = \sim_c^2 = \{(0,0), (1,1)\}$

- $pre_1(1) = q_b$ و $pre_1(0) = \neg q_b$

عمل واقع (N_2, y_b) است.

۳. عامل c رقم y_c را به طور خصوصی برای عامل a می فرستد.

عامل b نمی داند که آیا عامل c رقم 0 را فرستاده است یا رقم 1 را، و بین این دو موضوع مردد است. عمل شناختی زیر را برای مدل کردن این اعلان خصوصی در نظر می گیریم.

$$N_3 = \langle S_3, (\sim_i^3)_{i \in A}, pre_3 \rangle$$

- $S_3 = \{0,1\}$

- $\sim_b^3 = \{(0,0), (1,1), (0,1), (1,0)\}$ و $\sim_a^3 = \sim_c^3 = \{(0,0), (1,1)\}$

- $pre_1(1) = q_b$ و $pre_1(0) = \neg q_b$

عمل واقع (N_3, y_c) است.

مدل $(Dining, (x_a, x_b, x_c, y_a, y_b, y_c))$ را با عمل شناختی (N_1, y_a) به روز رسانی می کنیم.

سپس مدل حاصل $(Dining_1, (x_a, x_b, x_c, y_a, y_b, y_c))$ ، را با (N_2, y_b) به روز رسانی می کنیم و

مدل بدست آمده، $(\text{Dining}_2, (x_a, x_b, x_c, y_a, y_b, y_c))$ ، را با (N_3, y_c) به روز رسانی می‌کنیم.

مدل نهایی را با $(\text{Dining}_3, (x_a, x_b, x_c, y_a, y_b, y_c))$ نشان می‌دهیم.

می‌توان دید که مدل دانش Dining_3 بصورت زیر است. فضای حالت‌های ممکن Dining_3 می‌تواند همان فضای حالت‌های ممکن مدل Dining فرض شود و تابع ارزشدهی نیز مطابق با تابع ارزشدهی مدل Dining می‌باشد. تنها تفاوت در روابط است که بصورت زیر خواهند بود.

$$((x_a, x_b, x_c, y_a, y_b, y_c), (x'_a, x'_b, x'_c, y'_a, y'_b, y'_c)) \in R^3_a \Leftrightarrow x_a = x'_a \ \& \ y_a = y'_a \ \& \ y_c = y'_c$$

$$((x_a, x_b, x_c, y_a, y_b, y_c), (x'_a, x'_b, x'_c, y'_a, y'_b, y'_c)) \in R^3_b \Leftrightarrow x_b = x'_b \ \& \ y_b = y'_b \ \& \ y_a = y'_a$$

$$((x_a, x_b, x_c, y_a, y_b, y_c), (x'_a, x'_b, x'_c, y'_a, y'_b, y'_c)) \in R^3_c \Leftrightarrow x_c = x'_c \ \& \ y_c = y'_c \ \& \ y_b = y'_b$$

۴. عامل a مقدار $x_a + y_a + y_c$ را اعلان عمومی می‌کند. در حقیقت عامل a اگر مقدار

$x_a + y_a + y_c$ برابر 1 باشد گزاره زیر را اعلان عمومی می‌کند.

$$\vee_1 p_a \tilde{\vee} q_a \tilde{\vee} q_c$$

و اگر برابر 0 باشد گزاره

$$\neg(p_a \tilde{\vee} q_a \tilde{\vee} q_c)$$

را اعلان عمومی می‌کند.

⁷¹ نماد $\tilde{\vee}$ به این صورت تعریف می‌شود $p \tilde{\vee} q \equiv (p \vee q) \wedge \neg(p \wedge q)$.

۵. عامل b نیز با توجه به مقدار $x_b + y_b + y_a$ یا

$$p_b \tilde{V} q_b \tilde{V} q_a$$

را اعلان عمومی می کند یا گزاره

$$\neg(p_b \tilde{V} q_b \tilde{V} q_a)$$

را اعلان عمومی می کند.

۶. عامل c نیز با توجه به مقدار $x_c + y_c + y_b$ یا

$$p_c \tilde{V} q_c \tilde{V} q_b$$

را اعلان عمومی می کند یا گزاره

$$\neg(p_c \tilde{V} q_c \tilde{V} q_b)$$

را اعلان عمومی می کند.

اکنون اگر $(\text{Dining}_3, (x_a, x_b, x_c, y_a, y_b, y_c))$ را با سه اعلان عمومی ۴، ۵ و ۶ به روز رسانی کنیم

مدل نهایی Final-Dining (که بعد از اجرای پروتکل باید بدست آید) را خواهیم داشت.

مدل Final-Dining بصورت زیر خواهد بود

$$(x'_a, x'_b, x'_c, y'_a, y'_b, y'_c) \in S_F \Leftrightarrow (x'_a + y'_a + y'_c = x_a + y_a + y_c) \& (x'_b + y'_b + y'_a = x_b + y_b + y_a) \\ \& (x'_c + y'_c + y'_b = x_c + y_c + y_b)$$

تعداد حالت‌های ممکن برابر با تعداد جواب‌های معادله زیر با متغیرهای $x'_a, x'_b, x'_c, y'_a, y'_b, y'_c$ و ثوابت $x_a, x_b, x_c, y_a, y_b, y_c$ (به یاد آورید که حالت واقع $(x_a, x_b, x_c, y_a, y_b, y_c)$ و پروتکل بر اساس حالت واقع اجرا می‌شود) می‌باشد.

$$\begin{aligned}x'_a + y'_a + y'_c &= x_a + y_a + y_c \\x'_b + y'_b + y'_a &= x_b + y_b + y_a \\x'_c + y'_c + y'_b &= x_c + y_c + y_b \\x'_i x'_j &= 0 \text{ for all } i, j \in \{a, b, c\}\end{aligned}$$

تابع ارزش‌دهی همان تحدید شده تابع ارزش‌دهی Dining به فضای S_F است.

همچنین روابط مربوط به عاملها، همان روابط مدل Dining₃ است که به فضای S_F تحدید می‌شوند

یعنی

$$R^F_i = R^3_i \mid S_F \text{ برای } i \in \{a, b, c\}.$$

می‌توان بنابر دستگاه معادله فوق مشاهده کرد که برای هر $(x'_a, x'_b, x'_c, y'_a, y'_b, y'_c) \in S_F$ داریم

$$\begin{aligned}x'_a + x'_b + x'_c &= x_a + x_b + x_c \\x'_i x'_j &= 0 \text{ for all } i, j \in \{a, b, c\}\end{aligned}$$

نتیجه می‌گیریم که یا در همه حالت‌های S_F ، یکی از x'_i ‌ها برابر 1 است، یا در همه حالت‌های S_F ، همه x'_i ‌ها برابر 0 هستند. این یعنی اینکه یا همه حالت‌های S_F گزاره $p_a \vee p_b \vee p_c$ را ارضا می‌کنند یا همه حالت‌های S_F گزاره $\neg(p_a \vee p_b \vee p_c)$ را ارضا می‌کنند. به این ترتیب، با توجه به معناشناسی همه‌دانی مشترک (بخش ۳-۲ را ببینید)، شرط نهایی زیر در مدل نهایی به روز رسانی شده ارضا می‌شود.

$$(\text{Final-Dining}, (x_a, x_b, x_c, y_a, y_b, y_c)) \models C_{abc}(p_a \vee p_b \vee p_c) \vee C_{abc}(\neg p_a \wedge \neg p_b \wedge \neg p_c)$$

یعنی یا همه عامل‌ها با هم بطور مشترک می‌دانند که پرداخت کننده سازمان امنیت است یا همه عامل‌ها با هم بطور مشترک می‌دانند که پرداخت کننده یک از آنها است.

برای بررسی شرط نهایی گمنامی، یعنی نشان دادن

$$(\text{Final-Dining}, (x_a, x_b, x_c, y_a, y_b, y_c)) \models [p_a \rightarrow C_{abc}(\neg K_b p_a \wedge \neg K_c p_a)] \wedge [p_b \rightarrow C_{abc}(\neg K_a p_b \wedge \neg K_c p_b)] \wedge [p_c \rightarrow C_{abc}(\neg K_b p_c \wedge \neg K_a p_c)]$$

می‌توانیم از بررسی کننده مدل‌های دانش^{۷۲} استفاده کنیم.

برای مطالعه بیشتر در مورد توصیف گمنامی به کمک منطق شناختی مرجع [11] را ببینید.

۴-۵-۳ توصیف و درستیابی پروتکل‌ها با منطق شناختی

این که چگونه یک پروتکل را با منطق شناختی درستیابی کنیم را می‌توان به مراحل زیر تقسیم کرد.

۱. سیستم چند عاملی که پروتکل در آن انجام می‌شود را مشخص کنید. برای این کار مراحل زیر

باید انجام شود

الف: گزاره‌های اتمی سیستم را مشخص کنید

ب: عامل‌هایی که در سیستم شرکت می‌کنند را مشخص کنید.

۲. مدل کریپکی دانش آغازین سیستم را بسازید. برای این منظور مراحل زیر باید انجام شود

الف: حالت‌های ممکن سیستم را لیست کنید

ب: با توجه به میزان دسترسی هر عامل به اطلاعات سیستم مشخص کنید که چه

وضعیت‌هایی را هر عامل نمی‌تواند از یکدیگر تمیز دهد.

ج: مشخص کنید در هر وضعیت چه گزاره‌های اتمی برقرار هستند.

۳. عمل‌هایی که در پروتکل در نظر گرفته شده است را به کمک عمل‌های شناختی توصیف کنید.

۴. خاصیت مورد نظر را به کمک گزاره‌های منطق شناختی توصیف کنید.

مدل کریپکی دانش آغازین را با عمل‌های شناختی حاصل از پروتکل به روز رسانی کنید و در مدل‌های

کریپکی دانش بدست آمده گزاره‌های متناظر با خواص را درستیابی کنید.

تمرین

۱. مساله ۱-۱-۲ حاصلجمع و حاصلضرب (سارا و پارسا) را ببینید. گراف دانش (مدل کریپکی) را برای دو عامل پارسا و سارا رسم کنید.
۲. فرض کنید در مساله کودکان گلی، یکی از کودکان نابینا است ولی عینک دودی به چشم دارد و دو کودک دیگر نمی‌داند که او بینا است یا نابینا. گراف دانش را برای ۳ کودک در این حالت رسم کنید.
۳. بازی کارت‌های روسی را با ۵ کارت ۰، ۱، ۲، ۳، ۴ در نظر بگیرید که به عامل‌های a, b هر کدام دو کارت و به عامل c یک کارت داده شود. آیا می‌توانید پروتکلی برای این حالت بازی طراحی کنید؟ برای درستی پاسخ خود برهان بیاورید.
۴. پارادوکس اعدام شگفت آور را مدل کنید. آیا این پارادوکس با پارادوکس کلانتر معادل است؟ پاسخ خود را با یک روش منطقی بیان کنید.

مراجع

- [1] A. Bleeker and J. van Eijck. *The epistemics of encryption*, Proceedings LOFT 4, 2000.
- [2] F. Dechesne and Y. Wang. *Dynamic epistemic verification of security protocols: framework and case study*, Proceedings of the workshop Logic, Rationality and Interaction, China, 2007.
- [3] van Ditmarsch, H. *The russian cards problem: a case study in cryptography with public announcements*. Technical report, Department of Computer Science, University of Otago, 2002.
- [4] H. van Ditmarsch, W. van der Hoek, B. Kooi, **Dynamic Epistemic Logic**, Springer, 2008.
- [5] H. van Ditmarsch, *Kipping secret with public communication*, Department of computer science, University of Otago, Dunedin, 2002.
- [6] H. van Ditmarsch, W. van der Hoek, R. van der Meyden, J. Ruan, *Model checking Russian cards*, Electronic Notes in Theoretical Computer Science 149:105-123, 2006.
- [7] J. van Eijck, S. Orzan. *Epistemic Verification of Anonymity*, Electronic Notes in Theoretical Computer Science, Vol 168 , 2007.
- [8] R. Fagin, J.Y. Halpern, Y. M., and M. Vardi. **Reasoning about Knowledge**. The MIT Presss, Massachusetts Institute of Technology, 1995.

۵

منطق بازی

مقدمه

گوییم یک عامل سودجو است هرگاه به دنبال انجام کاری باشد که سود او را بیشتر می کند. دقت کنید، سودجو بودن این معنا نیست که عامل به دنبال آن است که سود رقیبان خود را کمتر کند یا کاری را انجام دهد که فاصله بین سود او و سود رقیبانش کمتر شود. برای مثال، فرض کنید که اگر کار a را انجام دهید به شما ۱۰۰ تومان و به رقیبتان ۳۰۰ تومان می رسد و اگر کار b را انجام دهید به شما ۸۰ تومان و به رقیبتان ۱۰ تومان می رسد. اگر شما یک عامل سودجو باشید (نه یک عامل حسود) هیچگاه کار b را به a ترجیح نمی دهید.

در نظریه بازی ها فرض می کنیم که عامل ها سودجو هستند و بنابر منطق شناختی عقلانی عمل می کنند. نظریه بازی ها به دنبال پاسخ پرسش زیر است.

پرسش: در یک سیستم چندعاملی، برای هر عامل یک مجموعه از استراتژی ها در نظر گرفته شده است. یک حالت ممکن پایانی سیستم عبارت است از حالتی از سیستم که هر عامل استراتژی خود را انجام داده باشد. در هر حالت پایانی، برای هر عامل سودی مشخص شده است. اکنون، با فرض سودجو و

منطقی بودن عامل ها کدام حالت پایانی اتفاق خواهد افتاد؟

آشنایی کوتاه با نظریه بازی‌ها

فرض کنید یک عامل (یک شرکت) بخواهد تصمیم‌گیری انجام دهد تا سود خود را بهینه کند. اگر این عامل در تعامل با عامل‌های دیگر باشد این بهینه‌سازی نمی‌تواند تنها به تصمیم او وابسته باشد. نظریه بازی‌ها به بهینه‌سازی هر عامل در یک سیستم چندعاملی می‌پردازد. یعنی

یک بازی یک مساله بهینه‌سازی چندعاملی است.

۵-۱ بازی‌های ایستا^{۷۳}

به بازی که در آن عامل‌ها بطور به همزمان تصمیم‌گیری می‌کنند بازی ایستا گوئیم. به این ترتیب، هر عاملی در زمان تصمیم‌گیری از تصمیم عامل دیگر خبر ندارد.

تعریف ۵-۱-۱. یک بازی با مجموعه عاملها $P = \{1, 2, \dots, n\}$ عبارت است از

$$G(P) = ((S_i)_{i \in P}, (\Pi_i)_{i \in P})$$

۱. برای هر عامل i ، S_i یک مجموعه متناهی است که آن را مجموعه استراتژی‌های ساده^{۷۴} عامل i می‌نامیم،

۲. برای هر عامل i ، $\Pi_i : S_1 \times S_2 \times \dots \times S_n \rightarrow \mathbb{R}$ تابع سود^{۷۵} عامل i است.

مقدار $\Pi_i(s_1, s_2, \dots, s_n)$ سود عامل i ، در زمانی که عامل ۱ استراتژی s_1 ، عامل ۲ استراتژی s_2 و ... عامل n ، استراتژی s_n را انجام دهد، است.

فرض می‌کنیم که در یک بازی توابع سود و مجموعه استراتژی‌ها بین عاملها همه‌دانی مشترک است.

مثال ۵-۱-۲. چند بازی

بازی زندانی‌ها. برای بازی زندانی‌ها (بخش ۲-۲-۲) داریم: $P = \{1, 2\}$

$S_1 = S_2 = \{C, D\}$ که C : اعتراف کردن و D : اعتراف نکردن است. تابع‌های Π_1, Π_2 به

کمک جدول زیر مشخص می‌شود

$1 \backslash 2$	D	C
D	-2, -2	-5, 0
C	0, -5	-4, -4

بازی جوجه. برای بازی جوجه (بخش ۲-۲-۴) داریم: $P = \{1, 2\}$ ، $S_1 = S_2 = \{C, D\}$ که

C : کنار کشیدن و D : کنار نکشیدن است. تابع‌های Π_1, Π_2 به کمک جدول زیر مشخص می‌شود

$1 \backslash 2$	D	C
D	-10, -10	+1, -1
C	-1, +1	0, 0

بازی شکار. دو شکارچی با هم به شکار می‌روند. هر شکارچی می‌تواند یا گوزن شکار کند یا خرگوش.

امکان شکار گوزن به تنهایی نیست. اما هر شکارچی می‌تواند یک خرگوش را به تنهایی شکار کند.

گوشت گوزن از گوشت خرگوش خوشمزه‌تر است. برای بازی شکار داریم: $P = \{1, 2\}$

$S_1 = S_2 = \{C, D\}$ که C : شکار خرگوش و D : شکار گوزن است. تابع‌های Π_1, Π_2 به کمک

جدول زیر مشخص می‌شود

$1 \backslash 2$	D	C
D	4, 4	0, 3
C	3, 0	3, 3

بازی مهر. زن و شوهری برای ماه عسل به شمال ایران رفته‌اند. یک روز عصر، تصمیم می‌گیرند که برای

تفریح از هتل بیرون بروند. زن دوست دارد با هم به کنار دریا بروند و مرد دوست دارد که با هم به

کافی‌شاپ بروند. آنها می‌توانند از هم جدا شوند و هر یک به جایی که علاقه دارد بروند ولی تنهایی کمتر

خوش می‌گذرد. برای بازی مهر داریم: $P = \{1, 2\}$ ، $S_1 = S_2 = \{C, D\}$ که C : کافی‌شاپ

رفتن و D : دریا رفتن است. تابع‌های Π_1, Π_2 به کمک جدول زیر مشخص می‌شود. کدام بازیکن

مرد و کدام بازیکن زن است؟

$1 \backslash 2$	D	C
D	3, 2	1, 1
C	0, 0	2, 3

تمرین. برای جدول بازی زیر یک داستان بنویسید.

$1 \backslash 2$	D	C
D	4, 4	2, 5
C	3, 5	3, 3

۵-۱-۳ حالت پارتو و تعادل نش

فرض کنید که $G(P) = ((S_i)_{i \in P}, (\Pi_i)_{i \in P})$ یک بازی با مجموعه عاملها $P = \{1, 2, \dots, n\}$

باشد. n تایی $(s_1, s_2, \dots, s_n) \in S_1 \times S_2 \times \dots \times S_n$

○ یک حالت پارتو است هرگاه n تایی دیگری نباشد که در آن سود یک عامل چون j بیشتر شود در حالیکه سود هیچ عامل دیگر کمتر نشود. یعنی حالت $(s'_1, s'_2, \dots, s'_n)$ و عامل j وجود ندارد که

$$\text{برای هر } i, \Pi_i(s'_1, s'_2, \dots, s'_n) \geq \Pi_i(s_1, s_2, \dots, s_n) \text{ و}$$

$$\Pi_j(s'_1, s'_2, \dots, s'_n) > \Pi_j(s_1, s_2, \dots, s_n)$$

○ یک حالت تعادل نش است هرگاه اگر یک عامل از استراتژی های عامل های دیگر انجام داده اند آگاه شود علاقه ای به تغییر استراتژی خود نداشته باشد. یعنی برای هر عامل i ، و هر

$$s'_i \in S_i$$

$$\Pi_i(s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n) \geq \Pi_i(s_1, s_2, \dots, s_{i-1}, s'_i, s_{i+1}, \dots, s_n)$$

مثال ۵-۱-۴. در بازی زندانی ها، حالت (C, C) تعادل نش و حالت (D, D) پارتو است.

تمرین. برای بازی ها جوجه و شکار و مهر تعادل نش و حالت پارتو را در صورت وجود مشخص کنید.

تعریف ۵-۱-۵. برای عامل i ، و استراتژی های $s_i, s'_i \in S_i$ ، گوییم s'_i اکیدا مغلوب s_i است

هرگاه برای هر $j \neq i$ و هر $s_j \in S_j$

$$\Pi_i(s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n) > \Pi_i(s_1, s_2, \dots, s_{i-1}, s'_i, s_{i+1}, \dots, s_n)$$

در یک بازی فرض بر این است که سود عاملها همه دانی مشترک است. همچنین فرض بر این است که این یک همه‌دانی مشترک بین عاملها است که هر عاملی عقلانی^{۷۷} عمل می‌کند. با این مفروضات عامل-ها استراتژی‌های مغلوب خود را حذف می‌کنند تا جواب بازی بدست آید

مثال ۵-۱-۶. (روش حذف با تکرار استراتژی مغلوب). بازی با جدول زیر را در نظر بگیرید

1-2	L	M	R
U	1, 0	1, 2	0, 1
D	0, 3	0, 1	2, 0

در آغاز بازیکن اول هیچ استراتژی مغلوبی ندارد. نه U مغلوب D است و نه D مغلوب U . ولی برای بازیکن دوم، R مغلوب M است. پس بازیکن دوم R را حذف می‌کند.

1-2	L	M
U	1, 0	1, 2
D	0, 3	0, 1

چون عقلانی بودن عاملها همه‌دانی مشترک است، بازیکن اول می‌داند که بازیکن دوم R را حذف کرده است. اکنون برای بازیکن اول، D مغلوب U است، و بازیکن اول D را حذف می‌کند.

1-2	L	M
U	1, 0	1, 2

بازیکن دوم از همه‌دانی مشترک بودن عقلانی بودن عاملها نتیجه می‌گیرد که بازیکن اول D را حذف کرده است. در این مرحله برای بازیکن دوم، استراتژی L مغلوب M است و بازیکن دوم L را نادیده می‌گیرد. جواب بازی (U, M) است.

1-2	M
U	1, 2

یعنی بازیکن اول استراتژی U و بازیکن دوم استراتژی M را بازی می‌کند.

تمرین. نشان دهید.

۱. اگر حذف با تکرار استراتژی‌های مغلوب توسط n بازیکن، تنها یک ترکیب $(s_1, s_2, \dots, s_n)$

را باقی بگذارد آنگاه این ترکیب یک تعادل نش است.

۲. اگر ترکیب $(s_1, s_2, \dots, s_n)$ تعادل نش باشد آنگاه از حذف با تکرار استراتژی‌های مغلوب

توسط بازیکن‌ها، حذف نمی‌گردد.

نکته. تعادل نش یک بازی حالتی است که بازی در تعادل قرار دارد. یک بازی ممکن است چندین

تعادل نش داشته باشد. اینطور نیست که یک تعادل نش حالتی از بازی است که حتما اتفاق خواهد

افتاد. بلکه از فرض سودجو بودن و منطقی عامل‌ها تنها بدست می‌آید که یک حالت پایانی برای بازی

باید در تعادل باشد (و یکی از تعادل‌های نش است).

مثال ۵-۱-۷ جدول بازی زیر را در نظر بگیرید

		P_2		
		L	M	R
P_1	U	1, 3	4, 2	2, 2
	C	4, 0	0, 3	4, 1
	D	2, 5	3, 4	5, 6

دقت کنید که (D, R) یک تعادل نش است. یعنی در حالت (D, R) هیچ عاملی دوست ندارد در

صورتی که عامل دیگر به حالت توافق وفادار باشد حالت را به هم بزند. اما با روش حذف استراتژی‌های

مغلوب هیچ حالتی حذف نمی‌شود.

آیا هر بازی تعادل نش دارد؟ بازی پالام پولوم پلیش را در نظر بگیرید. دو بازیکن همزمان دست راست خود را به جلو می‌آورند. هر بازیکن می‌تواند دستش را به رو (H) یا به پشت (T) روی میز بگذارد. اگر هر دو بازیکن روی دستهایشان همانند باشد بازیکن اول می‌برد وگرنه بازیکن دوم می‌برد. جدول سود بصورت زیر است.

1-2	H	T
H	$+1, -1$	$-1, +1$
T	$-1, +1$	$+1, -1$

این بازی تعادل نش ندارد مگر اینکه برای بازی استراتژی‌های مرکب^{۷۸} در نظر بگیریم.

تعریف ۵-۱-۸. فرض کنید S_i مجموعه استراتژی‌های ساده عامل i باشد. یک استراتژی مرکب برای عامل i یک تابع احتمال δ_i روی مجموعه S_i است. یعنی عامل i با احتمال $\sigma_i(s)$ استراتژی $s \in S_i$ را بازی می‌کند. با Σ_i مجموعه همه استراتژی‌های مرکب عامل i را نمایش می‌دهیم. تابع سود عاملها به روش امید ریاضی بدست می‌آید. برای $(\sigma_1, \sigma_2, \dots, \sigma_n) \in \Sigma_1 \times \Sigma_2 \times \dots \times \Sigma_n$

$$\Pi_i(\sigma_1, \sigma_2, \dots, \sigma_n) = \sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \dots \sum_{s_n \in S_n} \sigma_1(s_1) \sigma_2(s_2) \dots \sigma_n(s_n) (\Pi_i(s_1, s_2, \dots, s_n))$$

مثال ۵-۱-۹. در بازی پالام پولوم پلیش، بازیکن اول می‌تواند این استراتژی مرکب را بازی کند که با احتمال p دستش را رو (H) و با احتمال $1-p$ دستش را به پشت (T) جلو بیاورد. همچنین بازیکن دوم می‌تواند این استراتژی مرکب را بازی کند که با احتمال q دستش را رو (H) و با احتمال

$1 - q$ دستش را پشت (T) رو کند. می‌توان بررسی کرد که برای $\sigma_1 = (\frac{1}{2}, \frac{1}{2})$ و

$\sigma_2 = (\frac{1}{2}, \frac{1}{2})$ ، ترکیب (σ_1, σ_2) تعادل نش است. **با نوشتن نابرابری‌ها تعادل نش بودن (σ_1, σ_2) را**

بررسی کنید.

تمرین. با در نظر گرفتن استراتژی‌های مرکب برای بازی جوجه، بازی شکار و بازی مهر، تعادل نش‌های جدید پیدا کنید.

قضیه ۵-۱-۱۰. هر بازی با تعداد متناهی عامل که مجموعه استراتژی‌های ساده هر عامل متناهی است، دارای تعادل نش با در نظر گرفتن استراتژی‌های مرکب است.

کاربرد استراتژی مرکب در انتخابات. اگر در یک انتخابات بین دو کاندیدا مردد بودید، آیا حاضرید

که از استراتژی مرکب استفاده کنید و تاس بیندازید؟ اگر ۴۰ درصد به کاندید A و ۶۰ درصد به

کاندید B **اطمینان** دارید، روی ۴ کارت A و ۶ کارت B بنویسید و به تصادف یکی را بیرون بکشید و

با آن کارت به پای صندوق رای بروید.

تمرین. (روش بهترین پاسخ). جدول بازی زیر را در نظر بگیرید.

		P_2		
		L	M	R
P_1	U	1, 3	4, 2	2, 2
	C	4, 0	0, 3	4, 1
	D	2, 5	3, 4	5, 6

تنها تعادل نش برای استراتژی‌های ساده جفت (D, R) است. اما این جفت به روش حذف استراتژی-های مغلوب به دست نمی‌آید. اگر بازیکن‌ها بخواهند با استراتژی مرکب بازی کنند، چه استراتژی بازی خواهد شد؟

متغیرهای u, c, d ($u + c + d = 1$) برای عمل‌های U, C, D و متغیرهای l, m, r ($l + m + r = 1$) را برای عمل‌های L, M, N در نظر بگیرید. اگر در این بازی **بهترین استراتژی** بازیکن P_1 ، $\sigma_1^* = (u^*, c^*, d^*)$ ، یعنی بازی کردن عمل U با احتمال u^* ، عمل C با احتمال c^* ، و عمل D با احتمال d^* ، باشد آنگاه **بهترین پاسخ**^{۷۹} بازیکن P_2 به این استراتژی عبارت است از یافتن l, m, r بطوریکه مقدار زیر بیشینه شود.

$$f(l, m, r) = 3lu^* + 0 + 5ld^* + 2mu^* + 3mc^* + 4md^* + 2ru^* + rc^* + 6rd^* \quad (1)$$

همچنین اگر در این بازی **بهترین استراتژی** بازیکن P_2 ، $\sigma_2^* = (l^*, m^*, r^*)$ ، یعنی بازی کردن عمل L با احتمال l^* ، عمل M با احتمال m^* ، و عمل R با احتمال r^* ، باشد آنگاه **بهترین پاسخ** بازیکن P_1 به این استراتژی عبارت است از یافتن u, d, c بطوریکه مقدار تابع زیر بیشینه شود.

$$g(u, c, d) = l^*u + 4l^*c + 2l^*d + 4m^*u + 0 + 3m^*d + 2r^*u + 4r^*c + 5r^*d \quad (2)$$

از آنجا که هر دو بازیکن به دنبال بیشینه کردن سود خود هستند و این موضوع بین آنها همه‌دانی مشترک است، جواب بازی حل همزمان دو مساله بهینه‌سازی بالا است. یعنی **بهترین پاسخ** بازیکن P_2 ، یعنی l, m, r برحسب u^*, c^*, d^* برای بیشینه کردن (۱) محاسبه می‌شود. همچنین مقادیر

u, d, c بر حسب l^*, m^*, r^* برای بیشینه کردن (۲) محاسبه می‌شود و دو دستگاه بدست آمده حل می‌شود. با مشتق‌گیری جزئی از دو تابع f, g جواب بازی را محاسبه کنید.

تمرین.

۱. بازی پالام پولوم پلیش را با روش بهترین پاسخ حل کنید.
۲. نشان دهید اگر یک بازی را به روش بهترین پاسخ حل کنیم، چندیایی که بدست می‌آید یک تعادل نش است. آیا چندیایی بدست آمده منحصر به فرد است.

یک مطالعه موردی، پرونده هسته‌ای در شورای امنیت

فرض کنید که شورای امنیت بخواهد ایران را به خاطر مساله هسته‌ای تحریم کند. دو کشور چین و روسیه بخاطر منافع ملی خود، نفت و بازار ایران، ممکن است به ایران کمک کنند و از حق وتو خود برای جلوگیری از تحریم استفاده کنند. کفایت یکی از این کشورها تحریم را وتو کند تا جلوی تحریم گرفته شود. وتو کردن تحریم برای یک کشور هزینه رویارویی با اعضای دیگر شورا و از دست دادن همکاری اقتصادی با آنها را دربر خواهد داشت. بازی بصورت زیر خواهد بود.

$$P = \{Ru, Ch\}$$

مجموعه بازیکن‌ها

عمل H : کمک کردن به ایران،

DH : کمک نکردن با ایران.

p : مقدار سود دسترسی به نفت و بازار ایران را در صورت نبود تحریم

$2c$: هزینه رویارویی با اعضای دیگر شورای امنیت و کمک به ایران

توابع Π_{Ch}, Π_{Ru} به کمک جدول زیر مشخص می‌شوند.

$Ru \mid Ch$	H	DH
H	$p - c, p - c$	$p - 2c, p$
DH	$p, p - 2c$	$0, 0$

اگر حداقل یکی از دو کشور به ایران کمک کند آنگاه هر دو بخاطر نبود تحریم به بازار ایران دسترسی دارند. اگر هیچ‌کدام کمک نکنند آنگاه هیچ سودی نمی‌برند. هر دو کشور دوست دارند تا تحریم اتفاق نیفتد و به بازار ایران دسترسی داشته باشند ولی هزینه کردن نیز برای آنها خوشایند نیست، پس تصمیم نهایی خود را بطور همزمان (بازی استاتیک) می‌گیرند. با توجه به مقادیر p, c که باید از واقعیت آنها را استخراج کرد، چندین بازی متفاوت اتفاق خواهد افتاد، که تعادل‌نش‌های آنها را پیدا می‌کنیم و مشخص می‌کنیم که این تعادل‌نش‌ها چه آگاهی را به سیاست‌مداران ایرانی می‌رسانند.

۱. حالت $p \geq 2c$. در این حالت تعادل‌های نش ساده $(H, DH), (DH, H)$ است. این دو تعادل نش به روش حذف استراتژی‌های مغلوب بدست نمی‌آیند. با تساهل، می‌توان گفت که به هر حال یکی از این دو کشور به ما کمک می‌کند.

۲. حالت $c < p < 2c$. در این حالت تعادل نش ساده (DH, DH) است. هیچ‌کدام به ایران کمک نمی‌کنند، فریب وعده‌های آنها را نخورید. (آیا بازی تعادل نش مرکب دارد؟)

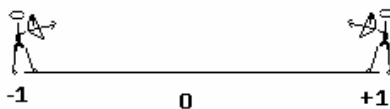
۳. حالت $p < c$. در این حالت نیز تعادل نش (DH, DH) است. اما این حالت از حالت ۲ بدتر است. اگر بازی، بازی تکرارشونده باشد در حالت ۲ امید به کمک کردن می‌رود ولی در حالت ۳ نه.

تمرین. در مدل سازی بالا، فرض کردیم که هر دو کشور روسیه و چین سود یکسانی، p ، از تحریم نشدن ایران می‌برند، و هزینه رویارویی، c ، با اعضای دیگر شورای امنیت نیز برای هر دو آنها یکسان است. بازی را برای حالتی که سودهای متمایز p_{Ru}, p_{Ch} هستند و هزینه‌ها نیز متمایز هستند مدل کنید و تعادل‌های نش مرکب و ساده را بدست آورید.

تمرین. به دور و بر خود نگاه کنید. یک مساله واقعی سیاسی-اجتماعی را در نظر بگیرید. ببینید که آیا آن یک بازی استاتیک است. جدول بازی را رسم کنید و تعادل‌های نش را بیابید.

تمرین. بازی سنگ، کاغذ، قیچی را در نظر بگیرید که دو کودک آن را بازی می‌کنند. سنگ بر قیچی پیروز است، قیچی بر کاغذ و کاغذ بر سنگ. اگر دو کودک شکل‌های یکسانی را پایین بیاورند بازی مساوی می‌شود. یک جدول بازی با فرض اینکه پیروزی امتیاز 1 و شکست امتیاز -1 دارد طراحی کنید و آن را حل کنید.

تمرین. بازی دوئل. خسرو و فرهاد می‌خواهند با هم دوئل کنند. خسرو روی نقطه 1- و فرهاد روی نقطه 1 ایستاده است. در دست هر کدام یک تیرکمان ساخته شده از شاخ گوزن است. دو نفر به هم نزدیک می‌شوند و تیری که در چله دارند را رها می‌کنند. هر نفر تنها یک تیر به همراه دارد، و اگر فردی تیر خود را زودتر از دیگری رها کند و به هدف نخورد طرف مقابل می‌تواند کامل به او نزدیک شود و تیر را در قلب او بزند. **احتمال برخورد تیر با فاصله دو رقیب نسبت عکس دارد.** در دو حالت زیر مشخص کنید که هر رقیب در چه نقطه‌ای به تیراندازی می‌پردازد.



۱. هر دو با قدم‌های گسسته به طول $\frac{1}{4}$ حرکت کنند. برای مثال، فرهاد از 1 به $\frac{3}{4}$ ، از $\frac{3}{4}$ به

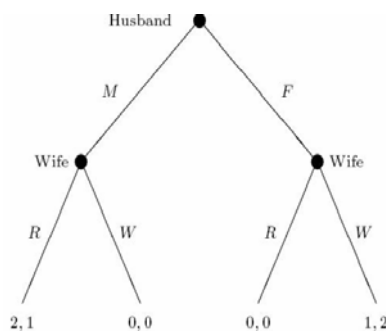
$\frac{2}{4}$ ، از $\frac{2}{4}$ به $\frac{1}{4}$ و بالاخره به صفر می‌رود.

۲. بطور پیوسته حرکت می‌کنند.

۵-۲ بازیهای دینامیک

بازی دینامیک بازی است که در آن بازیکن‌ها **نه ضرورتاً بطور همزمان** عمل خود را انجام می‌دهند. به این ترتیب، تصمیم‌هایی و استراتژی‌هایی که قبلاً اتخاذ شده‌اند **اعلان عمومی** می‌شوند و بازیکن‌ها در تصمیم‌های بعدی آن‌ها را در نظر می‌گیرند. توجه کنید که **بازی‌های استاتیک حالت خاصی از بازی‌های دینامیک هستند**. در یک بازی دینامیک ممکن است هم بعضی عملها همزمان و هم بعضی در زمان‌های جدا از هم انجام شوند.

برای مثال، بازی زیر یک بازی دینامیک است. زن w و شوهری h می‌خواهند مهمانی ترتیب دهند. شوهر قرار است گوشت M یا ماهی F بخرد و زن قرار است نوشابه W یا دلستر R بخرد. هر دو آنها دلستر را با گوشت و نوشابه را با ماهی دوست دارند. ولی شوهر گوشت را به ماهی و زن ماهی را به گوشت ترجیح می‌دهد. فرض کنید بازی استاتیک نیست. یعنی بطور همزمان خریدها صورت نمی‌گیرد و شوهر **خرید خود را انجام می‌دهد و به زنش می‌گوید که چه خریده است**. سپس زن به خرید می‌رود. درخت زیر بازی را نشان می‌دهد.



هر گره درخت به یک بازیکن تعلق دارد، و یالهایی که از آن گره خارج می‌شوند عمل‌هایی است که آن بازیکن می‌تواند انجام دهد. در برگ‌ها سود عاملها مشخص می‌شود. برای مثال اگر مسیر MR اجرا شود، یعنی شوهر گوشت قرمز بخرد و زن دلستر، آنگاه مرد ۲ امتیاز و زن ۱ امتیاز بدست می‌آورد.

تعریف ۵-۲-۱. **درخت بازی**. یک درخت بازی عبارت است از چندتایی

$$G = \langle P, N, (A_i)_{i \in P}, \varepsilon, \rightarrow, \nu, (\sim_i)_{i \in P}, n_0 \rangle$$

بطوریکه

۱. P یک مجموعه از بازیکن‌ها (عاملها) است.

۲. N مجموعه گره‌های گراف درختی است. (هر گره یا یک **گره تصمیم‌گیری** است که یک

بازیکن حق تصمیم‌گیری در آن دارد یا گره پایانی است)

۳. A_i یک مجموعه از عمل‌ها برای عامل i است.

۴. $\varepsilon : N - \text{Terminal}(N) \rightarrow P$ مشخص می‌کند که هر **گره تصمیم‌گیری** به کدام

بازیکن تعلق دارد. مجموعه $\text{Terminal}(N)$ برگ‌ها درخت است که در آن هیچ بازیکنی

تصمیم‌گیری نمی‌کند

۵. $\rightarrow : N \times \bigcup_{i \in P} A_i \rightarrow N$ یک تابع جزئی است که یالهای برچسب‌دار گراف را مشخص

می‌کند که باید خاصیت درخت بودن را حفظ کند. همچنین اگر $(n, a, m) \in \rightarrow$ آنگاه

$a \in A_{\varepsilon(n)}$. نماد $(n, a, m) \in \rightarrow$ را به صورت $n \xrightarrow{a} m$ نیز نمایش می‌دهیم.

۶. $\nu : \text{Terminal}(N) \times P \rightarrow \mathbb{R}$ تابعی است که مشخص می‌کند هر بازیکن (عامل) در

گره‌های پایانی چه سودی می‌برد.

۷. $\sim_i \subseteq N \times N$ یک رابطه هم‌ارزی است بطوریکه اگر $n \sim_i m$ آنگاه

$\varepsilon(n) = \varepsilon(m) = i$ رابطه $\sim_i$ مجموعه‌ای از گره‌ها را مشخص می‌کند که عامل i در

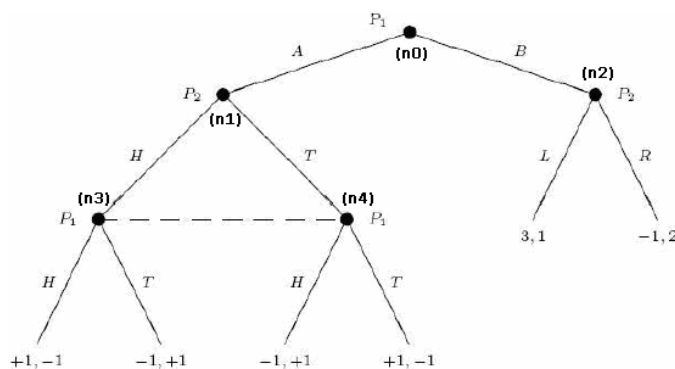
هنگام انجام بازی مردد است که در کدام گره قرار دارد.

۸. اگر $n, m \in \varepsilon^{-1}(i)$ و $n \sim_i m$ آنگاه برای هر $a \in A_i$ ، یالی با برچسب a از گره n

خارج می‌شود اگر و تنها اگر یالی با برچسب a از گره m خارج شود.

۹. n_0 گره آغازین بازی.

مثال ۵-۲-۲. درخت بازی زیر را ببینید.



خط چین رابطه هم‌ارزی $\sim_{P1}$ را نشان می‌دهد. ابتدا نوبت بازی $P1$ است که از یا عمل A را انجام

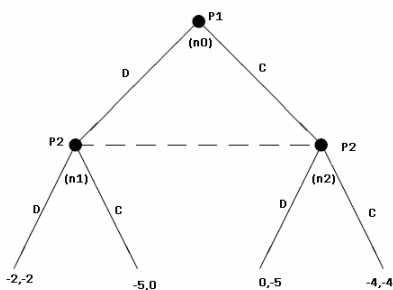
دهد یا عمل B را. اگر $P1$ عمل B را انجام دهد عامل $P2$ یا می‌تواند عمل L را انجام دهد یا

عمل R را. اگر $P1$ عمل A را انجام دهد و عامل $P2$ یا H را انجام می‌دهد یا T را. رابطه خط-

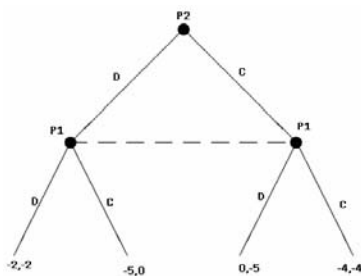
چین بین گره‌های $(n3), (n4)$ بیان می‌کند که عامل $P1$ از اینکه $P2$ کدام عمل H یا T را

انجام داده است آگاه نیست.

مثال ۵-۲-۳. درخت زیر بازی مساله زندانی‌ها است.



از آنجا که دو بازیکن $P1, P2$ همزمان عمل‌های خود را انجام می‌دهند، بازیکن $P2$ نمی‌تواند بین دو گرهی که با خط‌چین به هم وصل شده‌اند تمییز دهد. توجه کنید که درخت زیر نیز درخت بازی مساله زندانی‌ها است



تعریف ۵-۲-۴. درخت بازی $G = \langle P, N, (A_i)_{i \in P}, \varepsilon, \rightarrow, \nu, (\sim_i)_{i \in P}, n_0 \rangle$

۱. مجموعه استراتژی‌های ساده S_i برای بازیکن $i \in P$ عبارت است مجموعه همه توابع

$s : \varepsilon^{-1}(i) \rightarrow A_i$ بطوریکه برای هر گره $n \in \varepsilon^{-1}(i)$ گره $m \in N$ موجود است که

$(n, s(n), m) \in \rightarrow$ و اگر $n \sim_i t$ آنگاه $s(n) = s(t)$. تابع s مشخص می‌کند که

عامل i در گره‌هایی که نوبت او است چه عمل‌هایی را انجام می‌دهد. اگر عامل i نتواند دو گره

را از هم تمییز دهد آنگاه باید عمل‌های یکسانی در آنها انجام دهد. یک استراتژی مرکب برای

عامل i عبارت است از یک تابع که به هر گره تصمیم‌گیری متعلق به i ، یک توزیع احتمال نسبت می‌دهد که مشخص می‌کند هر یال خارج شده از گره با چه احتمالی بازی شود.

۲. تابع سود برای بازیکن $\Pi_i: S_1 \times S_2 \times \dots \times S_n \rightarrow \mathbb{R}, i \in P$ بصورت زیر مشخص می‌شود. برای محاسبه مقدار $\Pi_i(s_1, s_2, \dots, s_n)$ ، به این موضوع توجه کنید که استراتژی‌های ساده $s_1, s_2, \dots, s_n$ یک مسیر را از گره آغازین n_0 به یک گره پایانی چون m ایجاد می‌کنند. قرار می‌دهیم $\Pi_i(s_1, s_2, \dots, s_n) = v(m, i)$.

تمرین. استراتژی‌های ساده و مرکب بازیکن‌ها را برای درخت مثال ۵-۲-۲ بنویسید.

مثال ۵-۲-۵. در بازی زندانی‌های مثال ۵-۲-۳، درخت اول را در نظر بگیرید. داریم

$$\varepsilon^{-1}(P2) = \{n_1, n_2\} \text{ و } \varepsilon^{-1}(P1) = \{n_0\}$$

استراتژی‌های ساده عامل $P1$ عبارت است از دو استراتژی

$$1. \text{ تابع } D, s_{P1}^1(n_0) = D \text{ و}$$

$$2. \text{ تابع } C, s_{P1}^2(n_0) = C$$

استراتژی‌های ساده عامل $P2$ عبارت است از دو استراتژی

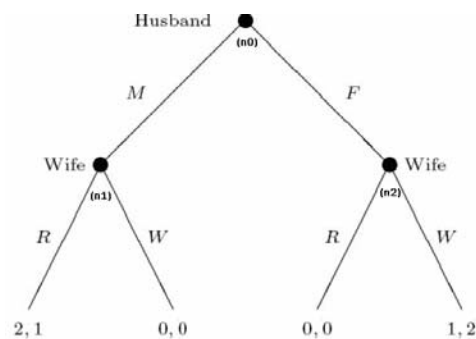
$$1. \text{ تابع } D, s_{P2}^1(n_1) = D, s_{P2}^1(n_2) = D \text{ و}$$

$$2. \text{ تابع } C, s_{P2}^2(n_1) = C, s_{P2}^2(n_2) = C$$

اگر توابع سود Π_1, Π_2 را از روی درخت بازی (بنابر تعریف ۵-۲-۴) حساب کنیم می‌توانیم جدول زیر را برای توابع سود بدست آوریم.

$1 \backslash 2$	$s_{P_2}^1$	$s_{P_2}^2$
$s_{P_1}^1$	$-2, -2$	$-5, 0$
$s_{P_1}^2$	$0, -5$	$-4, -4$

مثال ۵-۲-۶. استراتژی‌های ساده بازی زن و شوهر بصورت زیر است.



تنها گره n_0 متعلق به شوهر است و او تنها دو استراتژی دارد: یا ماهی بخرد یا گوشت قرمز، تابع

$$s_h^1(n_0) = M \text{ و } s_h^2(n_0) = F$$

اما زن چهار استراتژی بصورت زیر دارد. گره‌های n_1, n_2 متعلق به زن است.

۱. زن بدون توجه به این شوهرش چه خریده است، دلستر بخرد:

$$s_w^1(n_1) = R, s_w^1(n_2) = R$$

۲. زن بدون توجه به این شوهرش چه خریده است، نوشابه بخرد:

$$s_w^2(n_1) = W, s_w^2(n_2) = W$$

۳. اگر شوهر گوشت خرید، زن نوشابه بخرد و اگر ماهی خرید زن دلستر بخرد.

$$s_w^3(n_1) = W, s_w^3(n_2) = R$$

۴. اگر شوهر گوشت خرید، زن دلستر بخرد و اگر ماهی خرید زن نوشابه بخرد.

$$s_w^4(n_1) = R, s_w^4(n_2) = W$$

اگر توابع سود Π_1, Π_2 را از روی درخت بازی (بنابر تعریف ۵-۲-۴) حساب کنیم می‌توانیم جدول زیر را برای توابع سود بدست آوریم.

		W			
		s_w^1	s_w^4	s_w^3	s_w^2
H	s_h^1	<u>2</u> , <u>1</u>	<u>2</u> , <u>1</u>	0, 0	0, 0
	s_h^2	0, 0	1, <u>2</u>	0, 0	<u>1</u> , <u>2</u>

بررسی کنید تعادل‌های نش بازی برای استراتژی‌های ساده عبارتند از (s_h^1, s_w^1) ، (s_h^1, s_w^4) و (s_h^2, s_w^2) . تعادل‌های نش مرکب بازی را بیابید. اگر عامل‌ها عقلانی عمل کنند هیچگاه دو تعادل نش (s_h^1, s_w^1) و (s_h^2, s_w^2) اتفاق نمی‌افتند!!! زیرا، شوهر می‌داند که همسر او سودجو است و عقلانی عمل می‌کند و اگر او امروز گوشت بخرد، فردا که همسرش به خرید می‌رود دلستر را خواهد خرید. پس شوهر از بین ماهی و گوشت، خریدن گوشت را انتخاب می‌کند و آنچه اتفاق می‌افتد (s_h^1, s_w^4) است. به این روش حل بازی استقرای وارون گفته می‌شود.

حل بازی با استقرای وارون^{۸۰}. بازی‌های دینامیک را به روش استقرای وارون حل می‌کنیم. یعنی به روش استقرای وارون حالتی را که رخ خواهد داد پیش‌بینی می‌کنیم. فرض کنید که دو بازیکن 1 و 2 هر یک به ترتیب مجاز به انجام دادن عملیهایی از مجموعه‌های A_1 و A_2 هستند. بازیکن دوم در مرحله ۲ بازی مساله بهینه‌سازی

$$\max_{a_2 \in A_2} \Pi_2(a_1, a_2)$$

را که $a_1 \in A_1$ عملی است که بازیکن اول در گام پیش انتخاب کرده است را حل می‌کند. فرض کنید که برای هر $a \in A_1$ مساله بهینه‌سازی بالا دارای پاسخ منحصر به فرد $R_2(a)$ باشد. $R_2(a)$ بهترین عمل بازیکن دوم در برابر عمل بازیکن اول است. از آنجا که در یک بازی توابع سود **همه‌دانی مشترک** فرض می‌شوند، **بازیکن اول می‌تواند عمل بازیکن دوم را پیش‌بینی کند**. بنابراین هنگامی که بازیکن اول می‌خواهد در مرحله یک بازی، عمل خود را انتخاب کند با مساله بهینه‌سازی زیر روبرو است.

$$\max_{a \in A_1} \Pi_1(a, R_2(a))$$

فرض کنید که a_1^* پاسخ مساله فوق باشد آنگاه $(a_1^*, R_2(a_1^*))$ را پاسخ بازی بدست آمده از استقرای وارون می‌نامیم.

اگر مثال زن وشوهر را با استقرای وارون حل کنیم، پاسخ بازی (s_h^1, s_w^4) خواهد بود. دو تعادل نش دیگر بازی (s_h^1, s_w^1) و (s_h^2, s_w^2) اتفاق نمی‌افتند. در تعریف ۵-۲-۸ تعادل نش را بازبینی می‌کنیم تا با این تعریف فقط (s_h^1, s_w^4) بدست آید.

تعریف ۵-۲-۷. برای بازی دینامیک $G = \langle P, N, (A_i)_{i \in P}, \varepsilon, \rightarrow, \nu, (\sim_i)_{i \in P}, n_0 \rangle$ یک

زیربازی عبارت است از تحدید بازی به یک زیردرخت از گراف بازی بطوریکه

۱. گره شروع زیردرخت، n'_0 ، یکی از گره‌های **تصمیم‌گیری** (غیربرگ) بازی است بطوریکه بازیکن

$\varepsilon(n_0)$ بین این و گره دیگری مردد نیست. یعنی اگر $m \sim_{\varepsilon(n'_0)} n'_0$ آنگاه $n'_0 = m$.

۲. تمام گره‌های زیردرخت عبارتند از همه گره‌هایی که از n'_0 می‌توان به آنها رسید.

مثال ۵-۲-۸. بازی مثال ۵-۲-۲ را ببینید. این بازی ۳ زیربازی متفاوت دارد. زیربازی که از گره n_0

شروع می‌شود، زیربازی که از گره n_1 آغاز می‌شود، و زیربازی که از گره n_2 آغاز می‌شود.

بازی مثال ۵-۲-۳ تنها یک زیربازی دارد که همان خود بازی اصلی است و از گره n_0 آغاز می‌شود. **هر**

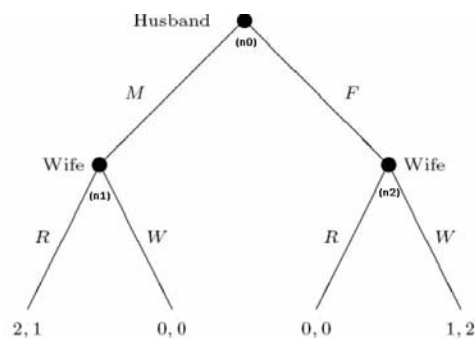
بازی استاتیک تنها یک زیربازی دارد که خود آن است.

تعریف ۵-۲-۹. یک تعادل‌نش زیردرخت-کامل^{۸۱} برای یک بازی دینامیک عبارت است از یک تعادل-نش

نش برای بازی بطوریکه برای هر زیربازی از بازی، تحدید استراتژی‌های این تعادل‌نش یک تعادل‌نش

برای زیربازی باشد.

مثال ۵-۲-۱۰. بازی زن و شوهر را در نظر بگیرید.



بازی دارای ۳ زیر بازی است. زیربازی که از n_0 آغاز می‌شود، زیربازی که از n_1 آغاز می‌شود، و زیربازی که از n_2 آغاز می‌شود. (s_h^1, s_w^1) یک تعادل نش زیربازی-کامل نیست. زیرا تحدید آن به زیربازی که از n_2 آغاز می‌شود یک تعادل نش برای این زیربازی نیست. در این زیربازی زن دوست دارد تا استراتژی خود را عوض کند. همچنین (s_h^2, s_w^2) یک تعادل نش زیربازی-کامل نیست. زیرا تحدید آن به زیربازی که از n_1 آغاز می‌شود، یک تعادل نش برای این زیربازی نیست. در این زیربازی زن دوست دارد تا استراتژی خود را از شراب سفید به شراب قرمز عوض کند. اما (s_h^1, s_w^4) یک تعادل نش زیربازی-کامل است.

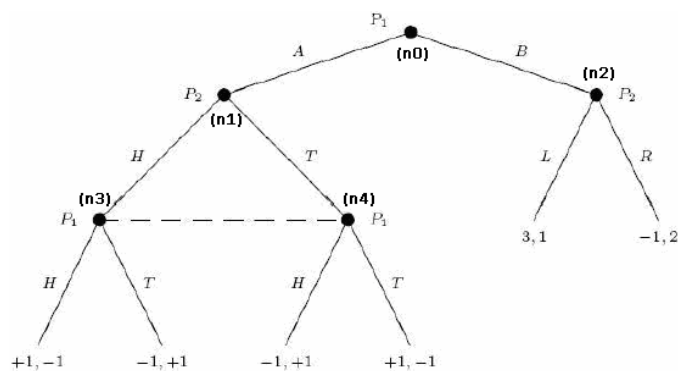
تمرین. نشان دهید

۱. اگر یک تعادل نش از استقرای وارون روی بازی بدست آید، آنگاه آن تعادل نش زیربازی-کامل است.

۲. هر بازی متناهی دینامیک دارای یک تعادل نش زیربازی-کامل است.

استقرای وارون گسترش یافته. در یک بازی دینامیک ممکن است که است که یک بازیکن مجموعه‌های تمییز ناپذیرش بیش از یک عضو داشته باشند. در این بازی‌های، از روش استقرای وارون

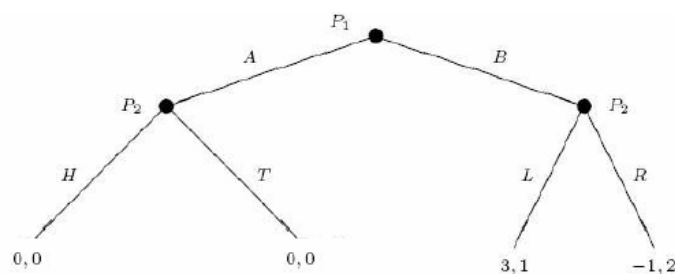
گسترش یافته استفاده می‌کنیم. درخت بازی زیر را در نظر بگیرید. بازیکن اول بین دو عمل A و B انتخاب می‌کند. اگر A انتخاب شود بازیکن اول و دوم بازی پالام پولوم پلیش را انجام می‌دهند. اگر B انتخاب شود بازیکن دوم بین دو عمل L و R انتخاب می‌کند.



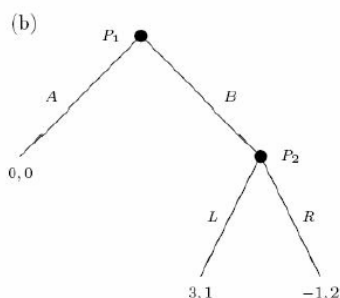
خط‌چین نشان می‌دهد که چون بازیکن اول و دوم همزمان پالام پولوم پلیش می‌کنند بازیکن اول بین دو گرهی که با خط‌چین به هم وصل شده‌اند نمی‌تواند تمییز دهد.

برای حل بازی فوق با استقرای وارون گسترش یافته بصورت زیر عمل می‌کنیم. در گره‌های n_3, n_4 ، بازیکن اول نمی‌داند که در واقع در کدام گره است، به همین دلیل عقلانی است که

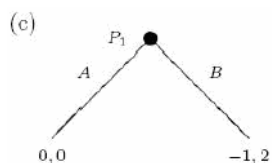
بصورت تصادفی با احتمال $\frac{1}{2}$ بازی می‌کند تا سود خود را بیشینه کند.



از آنجا که سودجو بودن و عقلانی بودن بازیکن اول یک همه‌دانی مشترک است، بازیکن دوم هم می‌داند که بازیکن اول به صورت تصادفی با احتمال $\frac{1}{2}$ بازی می‌کند. پس چه بازیکن اول H بازی کند چه T ، امید ریاضی سود برای هر دو برابر صفر است (درخت بالا و درخت پایین)



در گره n_2 ، بازیکن دوم برای بیشینه کردن سود خود R را انتخاب می‌کند. پس با استقرای وارون درخت بازی بصورت زیر می‌شود.



اکنون بازیکن اول A را انتخاب می‌کند. حل بازی اینگونه خواهد بود:

بازیکن اول A را انتخاب می‌کند و سپس بازیکن اول و دوم بازی پالام پولوم پلیش را با استراتژی حاصل از تعادل نش انجام می‌دهند.

تمرین. دزد دریایی ۵۰۰ سکه طلا پیدا می کنند. سلسله مراتب قدرت $A > B > C > D > E$ بین

دزدان وجود دارد. دزدان دریایی تصمیم می گیرند که بصورت زیر سکه ها را بین خود تقسیم کنند .

در هر مرحله عامل قویتر یک پیشنهاد برای تقسیم سکه ها می دهد و مشخص می کند که به هر

عاملی چند سکه از ۵۰۰ برسد . تقسیم به رای گذاشته می شود و اگر **حداقل** نصف آرا را بیاورد

پذیرفته می شود. اگر پیشنهاد پذیرفته شود، سکه ها تقسیم می شود و گرنه عامل قویتر را به داخل

آب می اندازد تا کوسه ها او را بخورند. سپس نوبت عامل قویتر بعدی می شود که پیشنهاد تقسیم

ارایه دهد فکر می کنید بازی به چه صورت انجام خواهد شد؟

حل بازی با استقرای وارون. اگر نوبت ارائه پیشنهاد به D برسد، یعنی A, B, C را کوسه خورده باشد، آنگاه دزد D

هیچ سکه ای به E نمی دهد. یعنی تقسیم به صورت $A = 0, B = 0, C = 0, D = 500, E = 0$ خواهد بود. اگر

نوبت ارائه پیشنهاد به C برسد. عامل C کفایت یک سکه به E بدهد تا عامل E به پیشنهاد رای بدهد. این بهترین

پیشنهادی است که E با آن روبرو خواهد شد. تقسیم به

صورت $A = 0, B = 0, C = 499, D = 0, E = 1$ خواهد بود. اگر نوبت ارائه پیشنهاد به B برسد. عامل B

کفایت یک سکه به D بدهد. تا **با رای خود** نصف آرا را بدست آورد.

$A = 0, B = 499, C = 0, D = 1, E = 0$ خواهد بود. عامل A پیشنهاد می کند که

$A = 498, B = 0, C = 1, D = 0, E = 1$ و پیشنهاد پذیرفته می شود.

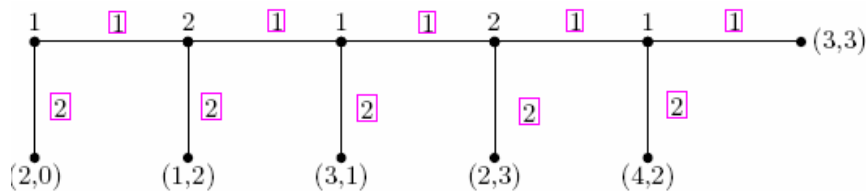
مساله ۲-۳-۹ دزدان دریایی را که در آن نحوه پذیرفته شدن رای متفاوت است، به روش استقرای

وارون حل کنید.

تمرین. یک بازی معرفی کنید که تعداد تعادل های نش زیربازی-کامل آن بیش از یکی باشد.

تمرین. درخت بازی هزارپا را برای شش اسکناس رسم کنید. استراتژی های بازیکن ها، تعادل های

نش بازی، و تعادل نش هایی که زیربازی-کامل هستند را مشخص کنید.



یک مطالعه موردی، پذیرش دموکراسی^{۸۲}.

یک سیستم اجتماعی را در نظر بگیرید که دو نوع عامل در آن وجود دارد ۱- عامل کارگر ۲- عامل سرمایه‌دار. فرض کنید که

(۱) $\lambda > \frac{1}{2}$ نسبت جمعیتی عامل‌های کارگر و $1 - \lambda$ نسبت جمعیت عامل‌های سرمایه‌دار باشد، و

(۲) درآمد عامل‌های سرمایه‌دار y^r و درآمد عامل‌های کارگر y^p باشد $y^p < y^r$.

درآمد متوسط جامعه $\bar{y} = \lambda y^p + (1 - \lambda)y^r$ است. آشکار است که $y^p < \bar{y} < y^r$.

(۳) پارامتر $\theta = \frac{\lambda y^p}{\bar{y}}$ سهم کارگری از درآمد متوسط جامعه را مشخص می‌کند. به راحتی

$$y^p = \theta \frac{\bar{y}}{\lambda}, \quad y^r = (1 - \theta) \frac{\bar{y}}{1 - \lambda} \quad \text{می‌توان دید}$$

در یک کشور دولت رفاه، دولت از عامل‌ها مالیات دریافت می‌کند و این مالیات را با خدماتی اجتماعی که ارائه می‌دهد، همانند تامین اجتماعی، امنیت، بهداشت و ...، دوباره به عامل‌ها بر می‌گرداند. فرض کنید

(۴) $\tau \in [0, 1]$ ، درصد مالیاتی باشد که عامل‌ها باید از درآمد خود بدهند (کسی که درآمد

بیشتری دارد از درصد بیشتری از خدمات اجتماعی، چون امنیت، استفاده می‌کند، پس به همان درصد مالیات بیشتری می‌دهد).

جمع آوری مالیات برای دولت هزینه دارد پس فرض کنید

(۵) $C(\tau)$ تابعی است که اگر دولت بخواهد $\tau \bar{y}$ مالیات جمع‌آوری کند آنگاه باید $C(\tau)\bar{y}$

$$C(\tau) = \frac{1}{2} \tau^2 \text{ هزینه کند. در اینجا فرض می‌کنیم}$$

به این ترتیب، دولت مقدار $(\tau - C(\tau))\bar{y}$ را خدمات اجتماعی به عامل‌ها می‌دهد. سود هر عامل، پس از پرداخت مالیات و دریافت خدمات اجتماعی برابر است با

$$V^p(\tau) = (1 - \tau)y^p + (\tau - \frac{1}{2}\tau^2)\bar{y}$$

$$V^r(\tau) = (1 - \tau)y^r + (\tau - \frac{1}{2}\tau^2)\bar{y}$$

هر عامل دوست دارد مقدار τ طوری تعیین شود که سود او بیشینه شود. تابع $V^r(\tau)$ مقدار بیشینه خود را در $\tau^r = 0$ می‌گیرد. سرمایه‌دارها دوست ندارند مالیات بدهند.

برای محاسبه نقطه بیشینه تابع $V^p(\tau)$ از آن مشتق بگیرید و برابر صفر قرار دهید.

$$V'^p(\tau) = -y^p + (1 - \tau)\bar{y} = 0$$

$$\tau^p = \frac{\lambda - \theta}{\lambda} \text{ داریم } \tau^p = \frac{\bar{y} - y^p}{\bar{y}} \text{ که بر حسب پارامتر } \theta, \text{ داریم}$$

از آنجا که کارگران درآمد کمتری از سرمایه‌داران دارند، سهم کارگری از درآمد متوسط، θ ، از سهم

آنها در جمعیت، λ ، کمتر است $\theta < \lambda$. پس کارگران دوست دارند که مقدار مثبت $\tau^p = \frac{\lambda - \theta}{\lambda}$

به عنوان مالیات در نظر گرفته شود. دقت کنید که هر چه سهم از درآمد متوسط، θ ، افزایش یابد

مقدار τ^p کاهش می‌یابد، این چه معنایی می‌دهد؟

در چه صورتی انقلاب کارگری چپ اتفاق می‌افتد؟ دو حالت انقلاب را در نظر بگیرید H : انقلاب

سخت، L : انقلاب نرم. در صورت انقلاب، به صنعت و اقتصاد یک کشور آسیب وارد می‌شود.

پارامترهای μ_H, μ_L را اینگونه در نظر بگیرید که اگر انقلاب سخت H اتفاق افتاد $1 - \mu_H$ از

اقتصاد نابود شود، و اگر انقلاب نرم L اتفاق افتاد $1 - \mu_L$ از اقتصاد نابود شود و فرض کنید

$$\mu_H < \mu_L$$

اگر انقلاب کارگری چپ اتفاق بیفتد هر چه از اقتصاد هست بین کارگران تقسیم می‌شود و سرمایه-

داران سودی نمی‌برند. برای $s \in \{L, H\}$

$$V^p(\text{Revolution}, \mu_s) = \frac{\mu_s \bar{y}}{\lambda}$$

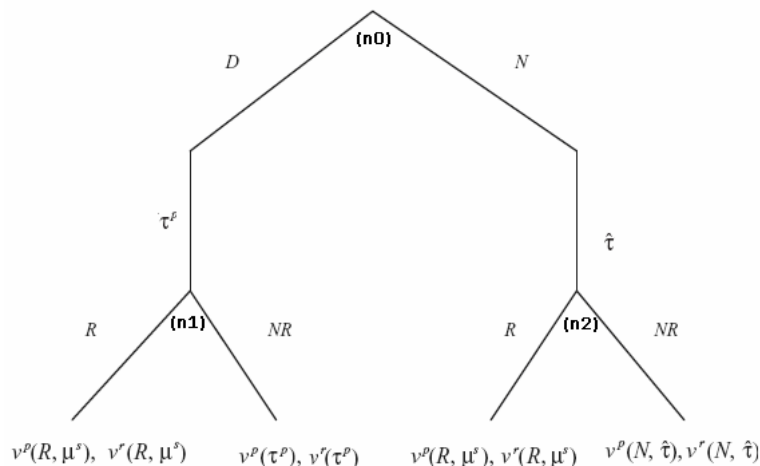
$$V^r(\text{Revolution}, \mu_s) = 0$$

اگر سرمایه‌دارها نخواهند مالیات بدهند و $V^p(\text{Revolution}, \mu_s) > V^p(0)$ آنگاه به سود کارگرها

است که انقلاب از نوع s را انجام دهند. با جایگزینی معادلات در نامساوی بالا به دست می‌آوریم

$\mu_s > \theta$. یعنی اگر θ ، سهم کارگری از درآمد متوسط جامعه، از μ_s کمتر باشد آنگاه انقلاب کارگری از نوع s اتفاق می‌افتد.

با توجه به مقدار سهم کارگری از درآمد متوسط جامعه و هزینه انقلاب، در آغاز آشکار می‌شود که قرار است انقلاب سخت اتفاق بیفتد یا انقلاب نرم. در این هنگام نوبت سرمایه‌دارها می‌شود که تصمیم بگیرند عمل D را انجام دهند، یعنی در یک فضای دموکراتیک مقدار مالیات مشخص شود (از آنجا که تعداد کارگرها بیشتر است، مقدار τ^p رای می‌آورد) و آن‌ها نیز مالیات را پرداخت کنند، یا آنک عمل N را انجام دهند یعنی سعی کنند که سیستم را کنترل کنند، از نفوذ خود در دولت استفاده کنند و مقدار $\hat{\tau}$ به عنوان مقدار مالیات مشخص کنند. سپس نوبت جامعه کارگری می‌شود که یا انقلاب کند R یا انقلاب نکند DR .



چگونه از انقلاب جلوگیری کنیم؟

در گره تصمیم‌گیری n_1 ، با آنکه سرمایه‌داران به τ^p تن در داده‌اند، اگر

$$V^p(\text{Revolution}, \mu_s) > V^p(\tau^p)$$

باز هم انقلاب رخ خواهد داد (متأسفانه، دیگر دیر شده است!). داریم

$$V^p(\text{Revolution}, \mu_s) > V^p(\tau^p) \text{ اگر و تنها اگر } \mu_s > \theta + \frac{(\lambda - \theta)^2}{2\lambda}$$

در این شرایط

برای سرمایه‌داران بهتر است عمل N را انجام دهند، شرایط را کنترل کنند و مقدار $\hat{\tau}$ را طوری انتخاب کنند که به انقلاب منجر نشود.

تمرین. تعادل‌های نش‌بازی را برای حالت‌های زیر پیدا کنید. توضیح دهید که معنای آنها چیست.

دست‌آورد کارگری انقلاب μ_s ،

سهم کارگری از درآمد متوسط جامعه θ ،

و سهم کارگری از جمعیت λ

الف. $\mu_s < \theta$.

ب. $\mu_s > \theta + \frac{(\lambda - \theta)^2}{2\lambda}$.

ج. $\theta < \mu_s < \theta + \frac{(\lambda - \theta)^2}{2\lambda}$.

تمرین. دو شرکت تجاری محصول یکسانی را تولید می‌کنند. قیمت محصول با توجه به فراوانی آن در بازار تعیین می‌شود، فرض کنید که اگر Q فراوانی محصول در بازار باشد قیمت محصول از تابع زیر

بدست می‌آید. $P(Q) = \begin{cases} P_0(1 - \frac{Q}{Q_0}) & Q < Q_0 \\ 0 & Q \geq Q_0 \end{cases}$ که در آن P_0 و Q_0 مقدارهای ثابت و مشخص

هستند. اگر بازار به حالت اشباع برسد قیمت به صفر می‌رسد. در صورت کمیابی محصول قیمت افزایش پیدا می‌کند. دو شرکت می‌خواهند برای سال آینده این محصول را تولید کنند. فرض کنید که q_1 مقدار محصولی باشد که شرکت ۱ تولید کند و q_2 مقدار محصولی باشد که شرکت ۲ تولید کند. قیمت برای مقدار $Q = q_1 + q_2$ محاسبه می‌شود. فرض کنید که هزینه تولید یک محصول برای هر دو شرکت برابر c باشد. آنگاه تابع سود شرکت $i \in \{1, 2\}$ به صورت زیر است.

$$\Pi_i(q_1, q_2) = q_i P(q_1 + q_2) - cq_i$$

$q_i P(q_1 + q_2)$ میزان فروش شرکت i ، و cq_i میزان هزینه کردن شرکت i است.

۱. اگر دو شرکت بطور همزمان محصول سال آینده خود را تولید کنند، مقدار q_1, q_2 چقدر خواهد بود.

۲. اگر دو شرکت با هم اتحادیه تشکیل دهند سود بیشتری می‌برند؟ آیا این کار اتفاق می‌افتد.

۳. فرض کنید بازی به صورت دینامیک انجام شود. ابتدا شرکت ۱ محصول خود را تولید کند و سپس شرکت ۲ محصول خود را تولید کند. مقدار q_1, q_2 چقدر خواهد بود.

۴. در پرسش فرض کردیم هزینه تولید برای هر دو شرکت یکسان است اگر هزینه تولید یک شرکت c_1 و دیگری c_2 باشد، به گزینه‌های ۱ و ۲ و ۳ پاسخ دهید.

۵-۳ بازی‌های تکرار شونده

تاکنون در بازی‌هایی که بررسی کردیم فرض کردیم که بازی فقط برای یکبار اجرا می‌شود. ولی اگر قرار باشد بازی بطور پشت‌سرهم برای زمان نامحدود تکرار شود، آنگاه عامل‌ها برای بهینه کردن سودشان استراتژی‌های متفاوتی را انتخاب می‌کنند. بازی زندانی‌ها را در نظر بگیرید.

$1 \backslash 2$	D	C
D	-2, -2	-5, 0
C	0, -5	-4, -4

فرض کنید که دو زندانی می‌دانند که بازی برای تعداد بار نامحدود تکرار خواهد شد. در اینصورت، اگر یک دزد همکار خود را بفروشد امکان **تلافی** برای همکار او در دفعات بعدی است. امکان تلافی در دفعات بعدی، دو دزد را ترغیب می‌کند که استراتژی دیگری بجای استراتژی که در آن، بازی فقط یکبار انجام می‌شد برگزینند. اینکه دو زندانی بخواهند در هر مرحله بازی تکرار شونده همان استراتژی (C, C) را بازی کنند با فرض عقلانی و سودجو بودن آنها سازگار نیست.

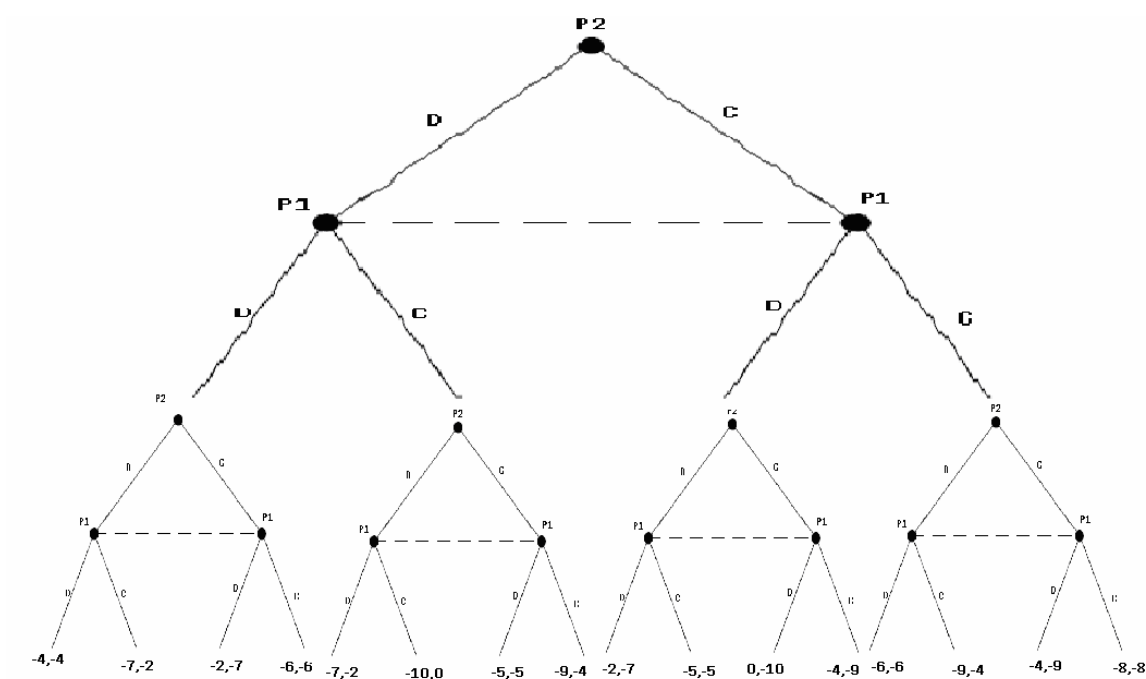
در بازی زندانی‌ها وقتی بازی یکبار انجام می‌شود زندانی‌ها **خیانت** را به **وفاداری** ترجیح می‌دهند، اما وقتی بازی بطور نامحدود تکرار شود، رفتار زندانی‌ها از خیانت به وفاداری تغییر می‌کند، زیرا امکان تلافی در دفعات بعدی برای هر بازیکنی هست.

بازی زندانی‌ها صورت‌های زیادی در اجتماع دارد، چون دو شرکت تجاری رقیب، زندگی زناشویی، سرمایه‌گذاری خصوصی-عمومی، دو حزب سیاسی جمهوری خواه و دمکرات و ... علت اینکه دو شرکت

رقیب اتحادیه تشکیل می‌دهد، زن و شوهر گذشت می‌کنند و احزاب سیاسی با هم همکاری می‌کنند و قدرت را به یکدیگر واگذار می‌کنند، این است که این بازی‌ها تکرارشونده هستند.

تمرین. نشان دهید اگر بازی زندانی‌ها فقط برای تعداد معین متناهی n بار (که عاملها از تعداد بار تکرار آگاهند) تکرار شود آنگاه در هر مرحله همان تعادل نش (C, C) بازی می‌شود.

تکرار n بار بازی زندانی‌ها یک بازی دینامیک خواهد بود که با استقرای وارون می‌توان نشان داد در هر مرحله هر بازیکن استراتژی C را بازی می‌کند. فرض کنید که بازی زندانی‌های دوبار تکرار شود. درخت بازی بصورت زیر خواهد بود.



با حل بازی به روش استقرای وارون خواهید تعادل نش این است که در هر دو مرحله (C, C) بازی شود.

فرض کنید که بازی زندانی‌ها نامتناهی بار تکرار شود. آیا باز هم در هر مرحله تکرار همان تعادل‌نش (C, C) بازی می‌شود؟ در اینجا امکان تلافی برای هر بازیکنی همیشه وجود دارد و مرحله آخری وجود ندارد.

تعریف ۵-۳-۱. یک بازی تکرار شونده $\text{Repeat}(G, \delta)$ عبارت است از یک بازی متناهی G که نامتناهی بار تکرار شود. مرحله k ام از بازی تکرار شونده، k امین تکرار بازی متناهی است. $0 < \delta < 1$ ضریب کاهنده بازی نام دارد (تعریف ۵-۳-۴ را ببینید).

برای بازی‌ها تکرار شونده، استراتژی‌های ساکن^{۸۳} را معرفی می‌کنیم.

تعریف ۵-۳-۲. یک استراتژی ساکن برای بازیکن i در یک بازی تکرار شونده $\text{Repeat}(G, \delta)$ ، یک دستورکلی ثابت برای انتخاب استراتژی است که می‌گوید در هر مرحله بازیکن i چه استراتژی را (از استراتژی‌های بازی متناهی G) انجام دهد. به عبارتی دیگر، یک استراتژی ساکن یک الگوریتم است که مشخص می‌کند در مرحله n ام با توجه به گذشته‌ای که رخ داده است چه عملی از بازی متناهی G باید انجام شود. مجموعه استراتژی‌های ساکن i را با $\bar{S}_i$ نمایش می‌دهیم

مثال ۵-۳-۳. استراتژی‌های زیر برای بازی تکرار شونده زندانی‌ها، استراتژی ساکن هستند.

▪ s^C : "همیشه C بازی کن." (همیشه اعتراف کن)

▪ s^D : "همیشه D بازی کن." (همیشه ساکت بمان)

▪ s^G : "اگر بازیکن مقابل در گذشته (درهیچ یک از مراحل قبل) C بازی نکرده است

(اعتراف نکرده است) D بازی کن (ساکت بمان)، وگرنه C بازی کن (اعتراف کن)." ^{۸۴}

(استراتژی بی بخشایش ^{۸۴})

▪ s^T : "در مرحله اول ساکت بمان (D)، در مراحل بعد همان کاری را بکن که بازیکن مقابل

در مرحله قبل انجام داده است." (استراتژی قصاص ^{۸۵})

دقت کنید که بازی زندانی‌ها یک بازی ایستا است و بازیکن‌ها در هر مرحله همزمان تصمیم‌گیری می‌-

کند ولی از آنچه در مراحل قبل انجام شده است آگاهند. همه استراتژی‌های بالا یک **دستورکلی ثابت**

است که مشخص می‌کند بازیکن باید در هر مرحله چگونه بازی کند.

تمرین. استراتژی‌های ساکن جدیدی برای بازی تکرارشونده زندانی‌ها معرفی کنید.

تعریف ۳-۴. بازی تکرار شونده $\text{Repeat}(G, \delta)$ با n بازیکن را در نظر بگیرید. برای هر

بازیکن i ، $\bar{s}_i \in \bar{S}_i$ یک استراتژی ساکن بازیکن i باشد. تابع سود به صورت زیر تعریف می‌شود

$$\bar{\Pi}_i(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n) = \sum_{t \in \mathbb{N}} r_i(t) \delta^t$$

که $r_i(t)$ سود بدست آمده از مرحله t ام است، و $0 < \delta < 1$ ، **ضریب کاهنده** ^{۸۶}، عددی است که از

دست رفتن ارزش سود در مراحل بعد را نشان می‌دهد.

در مورد δ سه نکته زیر را می‌توان بیان کرد

⁸⁴ Grim strategy

⁸⁵ Tit for Tat

⁸⁶ Discounting factor

۱. اگر ضریب δ را در تعریف ۳-۳-۵ لحاظ نکنیم آنگاه سری همگرا نخواهد بود

۲. δ میزان کم ارزش شدن سود دریافت شده در آینده است. ۱۰۰ هزار دلاری که امروز دریافت

می کنید ارزش بیشتری از ۱۰۰ هزار دلاری دارد که قرار است سال آینده دریافت کنید. (شما

می توانید ۱۰۰ هزار دلاری که امروز دارید را سرمایه گذاری کنید و سود یک سال آن را

بگیرید)

۳. می توان δ را احتمال ادامه پیدا کردن بازی دانست. در اینصورت تعداد مراحل تکرار قابل

انتظار (امید تعداد بار تکرار) برابر با $\frac{1}{1-\delta}$ خواهد بود. برای مثال اگر احتمال ادامه بازی

$$\delta = \frac{1}{2} \text{ باشد امید می رود که بازی برای 2 بار تکرار شود.}$$

مثال ۳-۵. بازی تکرار شونده زندانی ها را و استراتژی های ساکن مثال ۳-۳-۵ را در نظر بگیرید.

$$\bar{\Pi}_1(s^C, s^C) = \bar{\Pi}_2(s^C, s^C) = \sum_{t \in \mathbb{N}} -4\delta^t = \frac{-4}{1-\delta}$$

$$\bar{\Pi}_1(s^C, s^D) = \bar{\Pi}_2(s^D, s^C) = 0$$

$$\bar{\Pi}_1(s^D, s^C) = \bar{\Pi}_2(s^C, s^D) = \sum_{t \in \mathbb{N}} -5\delta^t = \frac{-5}{1-\delta}$$

$$\bar{\Pi}_1(s^G, s^G) = \bar{\Pi}_2(s^G, s^G) = \sum_{t \in \mathbb{N}} -2\delta^t = \frac{-2}{1-\delta}$$

$$\bar{\Pi}_1(s^D, s^G) = \bar{\Pi}_2(s^D, s^G) = \sum_{t \in \mathbb{N}} -2\delta^t = \frac{-2}{1-\delta}$$

$$\bar{\Pi}_1(s^C, s^G) = 0 + \sum_{t > 0} -4\delta^t = 4 + \frac{-4}{1-\delta}$$

اگر تنها سه استراتژی ساکن s^C, s^D, s^G را برای بازیکن‌ها در نظر بگیریم، و

$$s^C, s^D, s^G \text{ سه استراتژی این سه بازیکن با در نظر گرفتن این سه استراتژی } (s^G, s^G) \text{ باشد آنگاه } \frac{-2}{1-\delta} \geq 4 + \frac{-4}{1-\delta}$$

یک تعادل نش است. با ساده کردن نامساوی می‌تواند دید که باید ضریب کاهنده $\delta \geq \frac{1}{2}$ باشد.

تمرین. در بازی تکرارشونده زندانی‌ها استراتژی‌ها ساکن دو بازیکن را محدود به

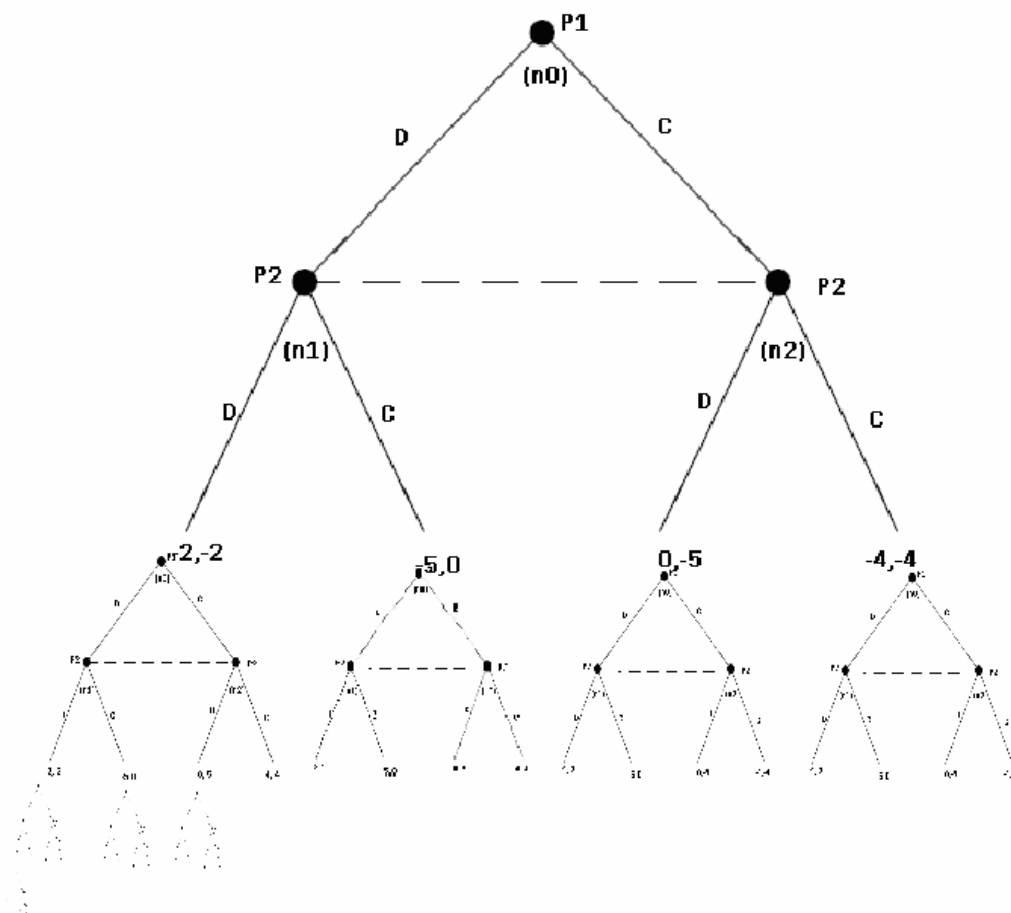
$$(s^T, s^T) \text{ کنید. ضریب کاهنده را طوری مشخص کنید که } \bar{s}_1 = \bar{s}_2 = \{s^C, s^D, s^G, s^T\}$$

تعادل نش شود.

بازی تکرار شونده $\text{Repeat}(G, \delta)$ را برای بازی متناهی G در نظر بگیرید. درخت بازی

$\text{Repeat}(G, \delta)$ عبارت است از تکرار نامتناهی بار درخت بازی G از برگها درخت G . برای مثال

اگر G بازی زندانی‌ها باشد درخت بازی $\text{Repeat}(G, \delta)$ به صورت زیر است.



یک زیر بازی از بازی $\text{Repeat}(G, \delta)$ ، زیر درختی است که از **گره آغازین** یکی از مراحل تکرار بازی G شروع می‌شود. **هر زیربازی یک بازی تکرار شونده با خود آن بازی یکریخت است.** هر زیر بازی با یک دنباله متناهی از عمل‌های بازیکن‌ها متناظر می‌شود که عبارت است از مسیری در درخت بازی-تکرارشونده که گره آغازین بازی اصلی را به گره آغازین زیر بازی متصل می‌کند. به این دنباله **گذشته** زیربازی می‌گوییم.

تعریف ۵-۳-۶. چندتایی $(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ از استراتژی‌های ساکن برای بازی $\text{Repeat}(G, \delta)$ با n بازیکن، را **تعادل‌نش زیربازی-کامل** گوئیم، هرگاه هر عامل i ، با هر **گذشته‌ای** از بازی، در صورتی که

عامل‌های دیگر استراتژی خود را تغییر ندهند، عامل i انگیزه‌ای برای تغییر استراتژی خود نداشته باشد. به عبارتی باید تعادل‌نش زیر بازی کامل مستقل از گذشته است.

مثال ۵-۳-۷. جفت (s^G, s^G) یک تعادل‌نش زیربازی-کامل نیست. زیرا فرض کنید که گذشته DC اتفاق افتاده باشد، یعنی، بازیکن اول ساکت‌مانده باشد (D) و بازیکن دوم اعتراف کرده باشد (C). در زیربازی با این گذشته، اگر بازیکن اول استراتژی s^G را انجام دهد باید در همه مراحل بعد اعتراف کند (C)، یعنی در این زیربازی برای بازیکن اول استراتژی s^G همان استراتژی s^C است. ولی بازیکن دوم، در این زیربازی، اگر استراتژی s^G را انجام دهد باید در مرحله بعد ساکت بماند (D) (چون در مراحل قبل، هنوز بازیکن اول اعتراف نکرده است) و سپس در مراحل بعد از آن اعتراف کند. اما با این گذشته، به سود بازیکن دوم نیست که مطابق استراتژی ساکن s^G بازی کند، بازیکن دوم انگیزه دارد که استراتژی ساکن s^D را برای این زیربازی در نظر بگیرد، و از همان مرحله اول زیربازی اعتراف کند تا سود بیشتری را بدست آورد.

تمرین. استراتژی ساکن

▪ s^g : "اگر در گذشته (درهیچ‌یک از مراحل قبل) C بازی نشده است (کسی اعتراف نکرده

است) D بازی کن (ساکت بمان)، وگرنه C بازی کن (اعتراف کن)."

را به جای استراتژی ساکن

▪ s^G : "اگر بازیکن مقابل در گذشته (درهیچ یک از مراحل قبل) C بازی نکرده است

(اعتراف نکرده است) D بازی کن (ساکت بمان)، وگرنه C بازی کن (اعتراف کن)."

در نظر بگیرید. نشان دهید که (s^g, s^g) یک تعادل نش زیربازی کامل برای بازی تکرارشونده زندانی‌ها است. (گذشته‌ها را می‌توانید به ۴ نوع مختلف تقسیم کنید. ۱- گذشته‌ای که در آن هیچکس C بازی نکرده است. ۲- گذشته‌ای که در آن هر دو بازیکن C بازی کرده‌اند. ۳- گذشته‌ای که بازیکن اول در آن C بازی کرده است ولی بازیکن دوم C بازی نکرده است. ۴- گذشته‌ای که بازیکن دوم در آن C بازی کرده است ولی بازیکن اول C بازی نکرده است. نشان دهید که در هر ۴ نوع، هیچکدام از عامل‌ها انگیزه‌ای برای تغییر استراتژی خود ندارند.)

در یک بازی تکرارشونده با n بازیکن، چگونه تشخیص دهیم که n تایی $(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ از استراتژی‌های ساکن یک تعادل نش زیربازی کامل است؟ دقت کنید که استراتژی‌های ساکن را محدود در نظر نگرفته‌ایم.

تعریف ۵-۳-۸. شرط انحراف یک مرحله‌ای^{۸۷}. چندتایی $(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ از استراتژی‌های ساکن برای بازی $\text{Repeat}(G, \delta)$ با n بازیکن، در شرط انحراف یک مرحله‌ای صدق می‌کند هرگاه برای هر عامل i ، اگر عامل‌های دیگر استراتژی خود را تغییر ندهند، عامل i انگیزه‌ای برای اینکه در یک مرحله از استراتژی ساکن خود منحرف شود و عملی دیگر انجام دهد و در مراحل بعد مطابق با استراتژی خود عمل کند نداشته باشد.

تمرین. ضریب کاهنده را طوری انتخاب کنید که (s^g, s^g) برای بازی تکرارشوند زندانی‌ها در شرط انحراف یک مرحله‌ای صدق کند.

$1 \backslash 2$	D	C
D	$-2, -2$	$-5, 0$
C	$0, -5$	$-4, -4$

پاسخ. در هر مرحله از بازی (گیرید مرحله n) دو نوع گذشته ممکن است. یا ۱- هر دو بازیکن D بازی کرده‌اند یا ۲- یکی از آنها C بازی کرده است.

۱. هر دو بازیکن D بازی کرده‌اند. استراتژی s^g مشخص می‌کند که باید در این مرحله نیز D بازی شود. فرض کنید که یکی از بازیکن در مرحله n از استراتژی s^g منحرف شود (تخطی کند) و C بازی کند و سپس مطابق با دستور استراتژی G در همه مراحل بعدی C بازی کند. (دقت کنید که بازیکن دیگر فقط در مرحله n ، D بازی می‌کند و در مراحل بعدی C بازی خواهد کرد) سود مورد انتظار این بازیکن از مرحله n به بعد برابر است با

$$0\delta^n + -4\delta^{n+1} + -4\delta^{n+2} + \dots = 0 + \delta^{n+1}\left(\frac{-4}{1-\delta}\right)$$

اگر بازیکن از استراتژی منحرف نشود، سود مورد انتظار او از مرحله n به بعد برابر است با

$$-2\delta^n + -2\delta^{n+1} + -2\delta^{n+2} + \dots = \delta^n\left(\frac{-2}{1-\delta}\right)$$

برای آنکه بازیکن انگیزه‌ای برای انحراف یک مرحله‌ای نداشته باشد باید

$$\delta^{n+1}\left(\frac{-4}{1-\delta}\right) \leq \delta^n\left(\frac{-2}{1-\delta}\right)$$

با حل نابرابری خواهیم داشت $\delta \geq \frac{1}{2}$.

۲. یکی از آنها C بازی کرده است. استراتژی s^g مشخص می کند که باید در این مرحله C بازی شود. فرض کنید که یکی از بازیکن در مرحله n از استراتژی s^g منحرف شود (تخطی کند) و D بازی کند و سپس مطابق با دستور استراتژی G در همه مراحل بعدی C بازی کند. (دقت کنید که بازیکن دیگر مطابق با استراتژی s^g همه مراحل بعد C بازی خواهد کرد) سود مورد انتظار این بازیکن از مرحله n به بعد برابر است با

$$-5\delta^n + -4\delta^{n+1} + -4\delta^{n+2} + \dots = -5\delta^n + \delta^{n+1}\left(\frac{-4}{1-\delta}\right)$$

اگر بازیکن از استراتژی منحرف نشود ، سود مورد انتظار او از مرحله n به بعد برابر است با

$$-4\delta^n + -4\delta^{n+1} + -4\delta^{n+2} + \dots = \delta^n\left(\frac{-4}{1-\delta}\right)$$

برای آنکه بازیکن انگیزه ای برای انحراف یک مرحله ای نداشته باشد باید

$$-5 + \delta^{n+1}\left(\frac{-4}{1-\delta}\right) \leq \delta^n\left(\frac{-4}{1-\delta}\right)$$

که برای هر مقداری برقرار است. پس کفایت که ضریب کاهنده $\delta \geq \frac{1}{2}$ باشد.

تمرین. نشان دهید n تایی $(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ از استراتژی های ساکن یک تعادل نش زیربازی کامل است اگر و تنها اگر در شرط انحراف یک مرحله ای صدق کند.

اگر تعادل نش در یک بازی استاتیک از **لحاظ اجتماعی مطلوب** نباشد، یعنی یک چندتایی از استراتژی-های بازیکن‌ها باشد که همه بازیکن‌ها در آن سود بیشتری از حالت تعادل نش می‌برند (برای مثال، بازی زندانی‌ها و سرمایه‌گذاری خصوصی-عمومی را ببینید)، آنگاه اگر بازی تکرار شود و ضریب کاهنده به اندازه کافی به ۱ نزدیک باشد بازیکن‌ها می‌توانند به سود بیشتری برسند. مثلاً بازی زندانی‌ها را در نظر بگیرید. حالت (C, C) از لحاظ اجتماعی مطلوب نیست چون در حالت (D, D) هر دو بازیکن سود بیشتری بدست می‌آورند. اگر بازی زندانی‌ها تکرار شوند و ضریب کاهنده $\delta \geq \frac{1}{2}$ باشد، بازیکن‌ها به سمت همکاری با همدیگر حرکت می‌کنند و سود بیشتری بدست می‌آورند.

تعریف ۵-۳-۹. فرض کنید G یک بازی استاتیک با n بازیکن باشد. **فضای سود شدنی بازی** عبارت

است از مجموعه n تایی‌های $(r_1, r_2, \dots, r_n)$ ، $r_i \in \mathbb{R}$ ، بطوریکه چندتایی $(s_1, s_2, \dots, s_n)$ از استراتژی‌های (مرکب) بازیکن‌ها باشد که برای هر i ، $\Pi_i(s_1, s_2, \dots, s_n) = r_i$.

مثال ۵-۳-۱۰. برای بازی استاتیک زندانی‌ها، **فضای سود بازی** عبارت است از مجموعه محدب بین

نقاط $(-2, -2), (0, -5), (-5, 0), (-4, -4)$.

تعریف ۵-۳-۱۱. بازی تکرارشونده $\text{Repeat}(G, \delta)$ را با n بازیکن در نظر بگیرید. با تعبیر δ به

عنوان امید ادامه بازی، تعداد بارهای قابل انتظار تکرار برابر با $T = \frac{1}{1-\delta}$ است. برای چندتایی

$(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ از استراتژی‌های ساکن، **سود متوسط بازیکن i در هر مرحله** را برابر با

$$\frac{1}{T} \bar{\Pi}_i(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$$

تعریف می‌کنیم. به $(z_1, z_2, \dots, z_n)$ ، $z_i \in \mathbb{R}$ ، سود متوسط شدنی گوییم هرگاه $(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ از

$$z_i = \frac{1}{T} \bar{\Pi}_i(\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n), \quad i \text{ هر برای که باشد}$$

تمرین. نشان دهید فضای سود شدنی بازی استاتیک G با فضای سود متوسط شدنی بازی $\text{Repeat}(G, \delta)$ یکسان است.

بازی تکرارشونده $\text{Repeat}(G, \delta)$ را با n بازیکن در نظر بگیرید. فرض کنید $(z_1, z_2, \dots, z_n)$ یک

سود متوسط شدنی بازی $\text{Repeat}(G, \delta)$ باشد. همچنین فرض کنید که $(r_1, r_2, \dots, r_n)$ سود

تبادل نش بازی استاتیک G باشد. اگر برای هر i ، $z_i > r_i$ ، آنگاه تکرار بازی سبب شده است تا همه عامل‌ها به سود بیشتری از سود تبادل نش برسند.

قضیه ۵-۳-۱۲.^{۸۸} فرض کنید $(r_1, r_2, \dots, r_n)$ سود یک تبادل نش بازی استاتیک G باشد و

$(v_1, v_2, \dots, v_n)$ یک سود شدنی بازی استاتیک G باشد بطوریکه برای هر i ، $v_i > r_i$. آنگاه عدد

$0 < \underline{\delta} < 1$ وجود دارد بطوریکه برای هر $\underline{\delta} < \delta < 1$ ، یک تبادل نش زیربازی کامل برای بازی

$\text{Repeat}(G, \delta)$ وجود دارد که $(v_1, v_2, \dots, v_n)$ سود متوسط شدنی آن باشد.

یک مطالعه موردی، همکاری دو حزب سیاسی رقیب

دو حزب سیاسی رقیب R و L را از یک کشور در نظر بگیرید. این دو حزب سیاسی می‌توانند هم

انحصارگر باشند و در پی حذف یکدیگر باشند، و هم می‌توانند با هم همکاری کنند. مسلماً اگر بازی

قدرت تکرارشونده نباشد، و تنها یکبار انجام شود، هر حزب به دنبال آن است که دیگری را حذف کند و برای این یکبار قدرت را بدست بگیرد. ولی اگر بازی تکرارشونده باشد، دو حزب سیاسی ممکن است به سمت همکاری با هم (و نه حذف یکدیگر) پیش بروند. این همکاری وابسته به ضریب کاهنده δ ، که در اینجا می تواند $\frac{1}{1-\delta}$ امید بقای نظام سیاسی تعبیر شود، است.

جدول زیر را برای بازی دو حزب در نظر بگیرید. استراتژی C همکاری کردن، و استراتژی D انحصار است.

L-R	C	D
C	(a,b)	(c,d)
D	(e,f)	(g,h)

برای جدول داریم

۱. $e > a, f < b$. (اگر حزب R همکاری کند حزب L ترجیح می دهد که انحصارطلبی کند،

و در این حالت حزب R متضرر می شود)

۲. $d > b, c < a$. (اگر حزب L همکاری کند حزب R ترجیح می دهد که انحصارطلبی کند،

و در این حالت حزب L متضرر می شود)

۳. $e > g, f < h$. (اگر L انحصارطلبی کند، حزب R نیز ترجیح می دهد که انحصارطلبی

کند، همچنین در همکاری R حزب انحصارطلب L سود بیشتری می برد)

۴. $h < d, c < g$. (اگر R انحصارطلبی کند، حزب L نیز ترجیح می دهد که انحصارطلبی

کند، همچنین در همکاری L حزب انحصارطلب R سود بیشتری می برد)

۵. $a > g, b > h$. هر دو حزب در همکاری دوطرفه سود بیشتری از انحصارطلبی دو طرفه

می‌برند.

همچنین فرض می‌کنیم که مقادیر جدول مثبت هستند. از ۵ گزینه بالا می‌توان بدست آورد که

$$e > a > g > c, d > b > h > f$$

برای بازی استاتیک بالا (D, D) تعادل نش است. بنابر قضیه ۵-۳-۱۲، $0 < \underline{\delta} < 1$ وجود دارد که اگر احتمال بقای نظام سیاسی (یعنی احتمال ادامه بازی دو حزبی) بیشتر از $\underline{\delta}$ باشد آنگاه سود متوسط شدنی (a, b) برای بازی تکرارشونده حاصل می‌شود.

استراتژی ساکن زیر را در نظر بگیرید.

s^g : "در هر مرحله از بازی در صورتی که در گذشته هیچ حزبی انحصارطلبی D نکرده است همکاری کن C ، و گرنه انحصارطلبی کن D ".

ضریب کاهنده δ را طور تعیین می‌کنیم که حالت (s^g, s^g) یک تعادل نش زیربازی کامل باشد. حالت (s^g, s^g) یک تعادل نش زیربازی کامل است هرگاه در شرط انحراف یک مرحله‌ای صدق کند. برای این منظور، فرض کنید که حزب L در مرحله n ام به تنهایی از استراتژی منحرف شود و دوباره مطابق استراتژی عمل کند.

$$\begin{array}{l} L : C \ C \ C \ C \ \dots \ \underset{n^{th} \ stage}{D} \ D \ D \ \dots \\ R : C \ C \ C \ C \ \dots \ \underset{n^{th} \ stage}{C} \ D \ D \ \dots \end{array}$$

سود L از مرحله n به بعد، در صورت انحراف یک مرحله‌ای از استراتژی، برابر است با

$$e\delta^n + g\delta^{n+1} + g\delta^{n+2} + \dots = e\delta^n + \delta^{n+1}\left(\frac{g}{1-\delta}\right)$$

سود L از مرحله n به بعد، در صورت عدم انحراف از استراتژی، برابر است با

$$a\delta^n + a\delta^{n+1} + a\delta^{n+2} + \dots = \delta^n\left(\frac{a}{1-\delta}\right)$$

اگر بخواهیم (s^g, s^g) در شرط انحراف یک مرحله‌ای صدق کند آنگاه باید

$$e\delta^n + \delta^{n+1}\left(\frac{g}{1-\delta}\right) \leq \delta^n\left(\frac{a}{1-\delta}\right)$$

با ساده کردن نامساوی بالا، برای آنکه حزب L انگیزه‌ای برای انحراف یک مرحله‌ای نداشته باشد، داریم

$$\delta \geq \frac{e-a}{e-g}$$

به همین ترتیب، می‌توان دید که برای آنکه حزب R انگیزه‌ای برای انحراف یک مرحله‌ای نداشته باشد،

باید

$$\delta \geq \frac{d-b}{d-h}$$

یعنی برای آنکه دو حزب مطابق با استراتژی s^g همکاری کنند، باید احتمال بقای نظام سیاسی بیشتر

از $\max\left(\frac{e-a}{e-g}, \frac{d-b}{d-h}\right)$ باشد.

اگر δ ، احتمال بقای نظام سیاسی، بیشتر از $\frac{e-a}{e-g}$ و کمتر از $\frac{d-b}{d-h}$ باشد، حزب L انگیزه‌ای

برای انحراف از استراتژی و عدم همکاری ندارد ولی حزب R علاقه‌مند به انحراف از همکاری و انحصارطلبی است.

فرض کنید که δ ، احتمال بقای نظام سیاسی، بیشتر از $\max(\frac{e-a}{e-g}, \frac{d-b}{d-h})$ باشد.

حتی با وجود این ممکن است انحصارطلبی اتفاق بیفتد.

برای حزب L داریم

$$e\delta^n + g\delta^{n+1} + g\delta^{n+2} + \dots \leq a\delta^n + a\delta^{n+1} + a\delta^{n+2} + \dots$$

از آنجا که $e > a$ ، حزب L با انحراف از استراتژی سود آنی‌اش بیشتر می‌شود و سپس به علت اینکه

$g < a$ است سودش کاهش پیدا می‌کند. قرار دهید $p_L(n)$ بزرگترین عددی باشد که

$$e\delta^n + g\delta^{n+1} + g\delta^{n+2} + \dots + g\delta^{p_L(n)} > a\delta^n + a\delta^{n+1} + a\delta^{n+2} + \dots + a\delta^{p_L(n)}$$

اگر حزب L در مرحله n از همکاری منحرف شود، تا مرحله $p_L(n)$ سودش بیشتر از سودی است

که در حالت همکاری بدست می‌آورد. فرض کنید هر مرحله بازی قدرت بین دو حزب در یکسال انجام

می‌شود. اگر $p_L(n) - n$ عددی بزرگ باشد، برای مثال ۳۰ سال، ممکن است حزب L به اندازه

کافی دوراندیش نباشد که بخواهد، سود بیشتری که در ۳۰ سال نصیب او می‌شود را رها کند تا در بیش

از ۳۰ سال متضرر نشود.

به همین ترتیب، قرار دهید $p_R(n)$ بزرگترین عددی باشد که

$$d\delta^n + h\delta^{n+1} + h\delta^{n+2} + \dots + h\delta^{p_R(n)} > b\delta^n + b\delta^{n+1} + b\delta^{n+2} + \dots b\delta^{p_R(n)}$$

اگر $p_R(n) - n$ عددی کوچک باشد، برای مثال ۴ سال، در حالیکه $p_L(n) - n$ عددی بزرگ

باشد، برای مثال ۳۰ سال، حزب R بیشتر از حزب L متمایل به همکاری است.

تمرین. تعبیری سیاسی برای مقادارهای $\frac{e-a}{e-g}$ و $\frac{d-b}{d-h}$ ارائه دهید.

مشاوره یک روانشناس خوب.

فرض کنید یک زن وشوهر به یک روانشناس خانواده مراجعه کردند. یک روانشناس از نگاه سیستم‌های اجتماعی کارهای زیر را انجام می‌دهد

۱. آگاهی توزیع شده بین زن و شوهر را به همه‌دانی مشترک تبدیل می‌کند، تا سوتفاهم‌ها برطرف شود.
۲. تعادل‌های نش را پیدا و آنها را به زن و شوهر توصیه می‌کند.
۳. تعهدات قانونی و اخلاقی را به تک تک آنها گوشزد می‌کند. همچنین آن دو را متوجه این موضوع می‌کند که همسر هر فرد به افراد دیگر جامعه نیز تعهداتی دارد که باید آنها را انجام دهد.
۴. آن دو را متوجه می‌کند که نمی‌توان بعضی کارها را همزمان انجام داد..
۵. به آنها می‌گوید که زندگی زناشویی یک بازی تکرارشونده است که امکان تلافی وجود دارد. بهترین استراتژی همکاری و گذشت دو طرف است.
۶.

۴-۵ بازی‌های ائتلافی

یک گروه از دزدان دریایی N را در نظر بگیرید که در دریا به دزدی از کشتی‌ها می‌پردازند. برای هر زیرمجموعه S از N ، بگذارید $\nu(S) \in \mathbb{R}$ مقدار پولی باشد، که اگر دزدان گروه S با هم متحد شوند، بتوانند در یکماه آن را با هم حاصل کنند.



توجه کنید که

۱. **ضرورتی ندارد که مقدار $\nu(S)$ مثبت باشد.** برای مثال، می‌تواند S گروهی شامل ۲ دزد باشد

که با هم دشمنی دارند و نمی‌توانند همدیگر را تحمل کنند. اگر این دو با هم به دزدی بپردازند، چون وقت بیشتر آنها در ماه صرف جنگیدن با یکدیگر می‌شود ممکن است حتی متضرر شوند.

۲. **ضرورتی ندارد که مقدار $\nu(S)$ برابر باشد با $\sum_{i \in S} \nu(i)$.** برای مثال، فرض کنید دزد i در

شمشیرزنی مهارت دارد و دزد j در تیراندازی. ائتلاف این دو با هم سبب می‌شود که در جنگیدن موفق‌تر باشند، و سود بیشتری از مجموع سودی که هر یک به تنهایی می‌برد حاصل شود.

اکنون فرض کنید یکی از دزدان دریایی بخواهد همه دزدها را با هم متحد کند. یعنی یک **ائتلاف اصلی**، N ، تشکیل دهد. پس از هر ماه دزدی باید پولها بین دزدهای داخل ائتلاف تقسیم شود. پرسش این است که

به هر دزد i چه بخشی از کالاهای دزدی شده (x^i) بدهیم که ائتلاف شکننده نباشد؟

تعریف ۵-۴-۱. یک بازی ائتلافی (برای افزایش سود) یک جفت (N, ν) است بطوریکه N مجموعه عاملها و $\nu : 2^N \rightarrow \mathbb{R}$ تابع ارزش ائتلافی است که $\nu(\emptyset) = 0$.

تعریف ۵-۴-۲. گوییم بازی ائتلافی (برای افزایش سود) (N, ν)

۱. **بالا-جمعی** است هرگاه برای هر $S, T \subseteq N$

$$(S \cap T = \emptyset) \Rightarrow \nu(S \cup T) \geq \nu(S) + \nu(T)$$

۲. **یکنوا** است هرگاه برای هر $S, T \subseteq N$

$$(S \subseteq T) \Rightarrow \nu(S) \leq \nu(T)$$

۳. **محدب** است هرگاه برای هر $S, T \subseteq N$

$$\nu(S \cup T) + \nu(S \cap T) \geq \nu(S) + \nu(T)$$

۴. **مقدار-ثابت** است هرگاه برای هر $S \subseteq N$ ، $\nu(S) + \nu(N - S) = \nu(N)$

۵. **صفر-نرمال** است هرگاه برای هر $i \in N$ ، $\nu(i) = 0$

مثال ۵-۴-۳. **حاجی‌ها و بازار**. یک بازار با m نوع کالا متمایز و مجموعه N از حاجی‌های

حجره‌دار را در نظر بگیرید.

برای هر $i \in N$ ، $a^i \in (\mathbb{R}^+)^m$ میزان موجودی کالاهای حاجی i ، در حال حاضر است.

برای هر $i \in N$ ، $w^i : (\mathbb{R}^+)^m \rightarrow \mathbb{R}$ یک تابع پیوسته است که تابع مطلوبیت حاجی i را

مشخص می‌کند. برای مثال، برای $x, y \in (\mathbb{R}^+)^m$ ، $w^i(x) > w^i(y)$ یعنی اینکه حاجی

ترجیح می‌دهد سبد x از کالاهای (یا سهام‌ها) را داشته باشد تا سبد y را.

فرض کنید $S \subseteq N$ یک مجموعه از حاجی‌ها باشد. یک معامله بین اعضای S عبارت است از

$$\sum_{i \in S} x^i = \sum_{i \in S} a^i \quad \text{بطوریکه} \quad x^i \in (\mathbb{R}^+)^m, \xi^i \in \mathbb{R}, (x^i, \xi^i)_{i \in S}$$

(میزان کل کالا پس از معامله تغییر نکرده است) و $\sum_{i \in S} \xi^i = 0$ (ξ^i پولی است که حاجی

i در معامله رد و بدل کرده است که باید مجموع صفر باشد). مجموعه X^S را عبارت از

همه $(x^i)_{i \in S}$ ، $x^i \in (\mathbb{R}^+)^m$ ، می‌گیریم که با انجام معامله بین اعضای گروه S (با شروع از

موجودی اولیه $(a^i)_{i \in S}$) می‌توان به آن رسید. بازی ائتلافی (N, ν) برای بازار بصورت زیر تعریف

می‌شود که ارزش ائتلاف S برابر است با

$$\nu(S) = \max \left\{ \sum_{i \in S} w^i(x^i) \mid (x^i)_{i \in S} \in X^S \right\}$$

تمرین. بررسی کنید که بازی ائتلافی بازار (مثال ۵-۴-۳) کدامیک از خصوصیات تعریف ۵-۴-۲ را

دارد.

بازی‌های ائتلافی را می‌توان به دو صورت نگاه کرد که دوگان هم هستند. ۱- ائتلاف برای افزایش سود ۲- ائتلاف برای کاهش هزینه. در بازی ائتلاف برای افزایش سود، عامل‌ها ائتلاف می‌کنند تا سود خود را بیشتر کنند، ولی در بازی ائتلاف برای کاهش هزینه، عامل‌ها ائتلاف می‌کنند تا هزینه خود را کمتر کنند.

تعریف ۴-۴-۵. یک بازی ائتلافی (برای کاهش هزینه) یک جفت (N, c) است بطوریکه N مجموعه عامل‌ها و $c : 2^N \rightarrow \mathbb{R}$ تابع هزینه ائتلافی است.

در بازی ائتلافی (برای کاهش هزینه)، یک بازیکن ائتلاف می‌کند تا هزینه کمتری بدهد و پول بیشتری ذخیره کند. به این ترتیب می‌توان هر بازی ائتلاف (برای کاهش هزینه) (N, c) را به یک بازی ائتلاف (برای افزایش سود) (N, ν) که برای هر $S \subseteq N$

$$\nu(S) = \sum_{i \in S} c(\{i\}) - c(S)$$

متناظر کرد.

تعریف ۵-۴-۵. گوییم بازی ائتلافی (برای کاهش هزینه) (N, c)

۱. **پایین-جمعی** است هرگاه برای هر $S, T \subseteq N$

$$(S \cap T = \emptyset) \Rightarrow c(S \cup T) \leq c(S) + c(T)$$

۲. **مقعر** است هرگاه برای هر $S, T \subseteq N$

$$c(S \cup T) + c(S \cap T) \geq c(S) + c(T)$$

مثال ۵-۴-۶. فرض کنید N یک مجموعه از شهرها باشند که می‌خواهند سیستم تامین آب شهری بسازند. برای تابع $c : 2^N \rightarrow \mathbb{R}$ و $S \subseteq N$ هزینه ساخت سیستم تامین آب به صورت گروهی است.

مثال ۵-۴-۷. یک بازی ائتلافی (N, ν) را ساده گوئیم هرگاه برای هر $S \subseteq N$ ، یا $\nu(S) = 0$ یا $\nu(S) = 1$ باشد. اگر $\nu(S) = 1$ ، گوئیم ائتلاف S یک ائتلاف برنده است، و اگر $\nu(S) = 0$ گوئیم ائتلاف S یک ائتلاف بازنده است.

۱. **عامل وتو:** در بازی ساده (N, ν) ، عامل $i \in N$ ، عامل وتو است هرگاه هر ائتلافی که شامل i نباشد یک ائتلاف بازنده باشد.

۲. **عامل دیکتاتور:** در بازی ساده (N, ν) ، عامل $i \in N$ ، عامل دیکتاتور است هرگاه هر ائتلافی که شامل i نباشد یک ائتلاف بازنده باشد و هر ائتلافی که شامل i باشد یک ائتلاف برنده باشد.

۳. **عامل نفرین شده:** در بازی ساده (N, ν) ، عامل $i \in N$ ، عامل نفرین شده است هرگاه هر ائتلافی که شامل i باشد یک ائتلاف بازنده باشد.

۴. **عامل کارا:** در بازی ساده (N, ν) ، عامل $i \in N$ ، عامل کارا است هرگاه هر ائتلافی که شامل i باشد یک ائتلاف برنده باشد.

۵. بازی ساده (N, ν) را رسمی گوئیم هرگاه متمم هر ائتلاف برنده، بازنده باشد.

۶. بازی ساده (N, ν) را **رسمی قطعی** گوییم هرگاه یک ائتلاف برنده باشد اگر و تنها اگر متمم آن بازنده باشد.

تمرین. برای تعریف‌های زیر نام‌گذاری مناسب کنید.

عامل ----: در بازی ساده (N, ν) ، عامل $i \in N$ ، عامل ---- است هرگاه هر ائتلافی که شامل i نباشد یک ائتلاف برنده باشد و هر ائتلافی که شامل i باشد یک ائتلاف بازنده باشد.

عامل ----: در بازی ساده (N, ν) ، عامل $i \in N$ ، عامل ---- است هرگاه هر ائتلافی که شامل i نباشد یک ائتلاف برنده باشد.

چند نمونه از سیستم‌های اجتماعی که در آن هستید را نام ببرید و مشخص کنید که در آنها چه نوع عاملی هستید.

در بازی دزدهای دریایی گفتیم که پرسش اصلی بازی‌های ائتلافی این است که چگونه سود حاصل از ائتلاف را بین عاملهای ائتلاف بخش‌بندی کنیم بطوریکه هیچ عاملی یا دسته‌ای از آنها انگیزه-ای برای شکستن ائتلاف نداشته باشد. تعریف زیر به این موضوع می‌پردازد.

تعریف ۵-۴-۸. (بردار بخش‌بندی) $\langle x_i \rangle_{i \in N}$ ، برای $x_i \in \mathbb{R}$ ، یک بردار بخش‌بندی برای

بازی ائتلافی (N, ν) است هرگاه $\sum_{i \in N} x_i \leq \nu(N)$.

۱. بردار بخش‌بندی $\langle x_i \rangle_{i \in N}$ **کارا** است هرگاه همه سود ائتلاف بخش‌بندی شود

$$\sum_{i \in N} x_i = \nu(N)$$

۲. بردار بخش‌بندی $\langle x_i \rangle_{i \in N}$ **سود ده فردی** است هرگاه سهم هر عامل از سودی که او می-

تواند به تنهایی بدست آورد کمتر نباشد $(\forall i \in N (x_i \geq \nu(\{i\})))$.

۳. بردار بخش‌بندی $\langle x_i \rangle_{i \in N}$ **متقارن** است هرگاه دو عامل با توانایی یکسان سهم برابری را

از بخش‌بندی بگیرند. یعنی، برای دو عامل $i, j \in N$ ، اگر برای هر

$$x_i = x_j \text{ آنگاه } \nu(S \cup \{i\}) = \nu(S \cup \{j\}), S \subseteq N - \{i, j\}$$

یک **بردار پاسخ** برای بازی عبارت از یک بردار بخش‌بندی کارا سودده فردی است. مجموعه بردارهای

پاسخ یک بازی را با T نمایش می‌دهیم

تعریف ۵-۴-۹. بازی ائتلافی (N, ν) و دو بردار بخش‌بندی $\langle x_i \rangle_{i \in N}, \langle y_i \rangle_{i \in N}$ را در نظر

بگیرید. گوییم بردار بخش‌بندی $\langle x_i \rangle_{i \in N}$ بر $\langle y_i \rangle_{i \in N}$ **غلبه** دارد هرگاه ائتلاف غیر تهی $S \subseteq N$

باشد بطوریکه برای هر $i \in S$ ، $x_i > y_i$ و $\sum_{i \in S} x_i \leq \nu(S)$. به عبارتی دیگر، بازیکن‌های

مجموعه S بردار پاسخ $\langle x_i \rangle_{i \in N}$ را بر $\langle y_i \rangle_{i \in N}$ ترجیح می‌دهند و اگر هم بخواهند می‌توانند با هم

ائتلاف کنند و سودی بدست بیاورند که بتوان بردار بخش‌بندی $\langle x_i \rangle_{i \in S}$ را در زیرگروه خود محقق

کنند.

تعریف ۵-۴-۱۰. برای بازی ائتلافی (N, ν) یک **مجموعه پایدار** $J \subseteq T$ از بردارهای پاسخ

مجموعه‌ای است که

الف: برای هر $\langle x_i \rangle_{i \in N}, \langle y_i \rangle_{i \in N} \in J$ ، نه $\langle x_i \rangle_{i \in N}$ بر $\langle y_i \rangle_{i \in N}$ غلبه دارد و نه $\langle y_i \rangle_{i \in N}$ بر

$$\langle x_i \rangle_{i \in N}$$

ب: برای هر $\langle y_i \rangle_{i \in N} \in T - J$ ، بردار $\langle x_i \rangle_{i \in N} \in J$ که $\langle x_i \rangle_{i \in N}$ بر $\langle y_i \rangle_{i \in N}$ غلبه دارد.

تعریف ۵-۴-۱۱. **هسته** بازی ائتلافی (N, ν) ، مجموعه $C \subseteq T$ است که

$$C = \left\{ \langle x_i \rangle_{i \in N} \in T \mid \forall S \subseteq N \left(\sum_{i \in S} x_i \geq \nu(S) \right) \right\}$$

تمرین. بازی دزدان دریایی را برای ۳ دزد $N = \{a, b, c\}$ در نظر بگیرید. در هر یک از حالت‌های زیر، مجموعه‌های پایدار، هسته بازی، و بردارهای پاسخ متقارن را مشخص کنید.

۱. تابع سود ائتلافی ν طوری است که فقط در صورتی که هر ۳ دزد با همدیگر همکاری

$$\text{کنند } \nu(N) = 6 \text{ و برای هر } S \subseteq N \text{ که } S \neq N, \nu(S) = 0$$

۲. تابع سود ائتلافی ν طوری است که حضور عامل a اساسی است.

$$\nu(N) = 6, \nu(\{a\}) = \nu(\{b\}) = \nu(\{c\}) = \nu(\{c, b\}) = 0 \text{ و}$$

$$\nu(\{a, b\}) = \nu(\{a, c\}) = 4$$

تمرین. نشان دهید هسته یک بازی زیر مجموعه هر مجموعه پایدار بازی است، و اگر هسته بازی خود یک مجموعه پایدار باشد آنگاه هسته تنها مجموعه پایدار منحصر به فرد بازی است.

تمرین. بازی دزدان دریایی را برای ۳ دزد $N = \{a, b, c\}$ در نظر بگیرید.

۱. تابع سود ائتلافی ارائه دهید که ائتلاف اصلی نتواند شکل بگیرد. یعنی هسته بازی تهی باشد.

۲. تابع سود ائتلافی ارائه دهید که هسته بازی بیش از یک عضو داشته باشد.

۳. تابع سود ائتلافی ارائه دهید که بازی مجموعه پایدار نداشته باشد.

یک مطالعه موردی، توصیف توزیع قدرت در سیستم‌های اجتماعی

هرگاه اجتماعی انسانی شکل می‌گیرد موقعیت قدرتی در آن بوجود می‌آید تا بعضی از نیازهای اجتماعی چون امنیت برآورده شود. قدرت چیزی است که از تاب انسان خارج است و خیلی زود گوهر انسانی فرد را پست و بی‌مایه می‌کند. اگر انسانی برای مدتی طولانی بر تخت قدرت تکیه بزند کم‌کم برای خود مقام ربوبیت قائل می‌شود و همچون نمرود می‌پندارد که می‌تواند انسانی را مورد عفو قرار دهد یا حکم پایان زندگی انسانی دیگر را صادر کند. فرعون نیز به این بیماری مبتلا شد وقتی گفت: "انا ربکم اعلا". فرعون ادعای آفرینندگی نمی‌کرد بلکه ادعا پرودگاری و ربوبیت داشت.

در زیر سیستم‌های اجتماعی را با توجه به نوع توزیع قدرت در آنها به کمک بازی‌های ائتلافی توصیف می‌کنیم.

حکومت تام: در این سیستم‌های اجتماعی همه قدرت اجتماع به یک فرد واگذار می‌شود. اگر حاکم به خواسته‌ای اجتماعی مایل باشد آن خواسته برآورده می‌شود و اگر به خواسته‌ای اجتماعی مایل نباشد آن خواسته هیچ‌گاه برآورده نخواهد شد. یعنی یک ائتلاف اجتماعی (یک خواسته اجتماعی) برنده است اگر و تنها اگر حاکم عضو آن ائتلاف باشد.

حکومت مشروطه: در این سیستم‌های اجتماعی قدرت بطور مشروط به یک فرد واگذار می‌شود. اگر حاکم به خواسته‌ای اجتماعی مایل باشد آن خواسته برآورده می‌شود به شرط آنکه مورد تایید مردم باشد، و اگر به خواسته‌ای اجتماعی مایل نباشد آن خواسته هیچ‌گاه برآورده نخواهد شد. یعنی یک ائتلاف اجتماعی (یک خواسته اجتماعی) برنده است اگر و تنها اگر آن ائتلاف شامل حاکم و اکثریت باشد.

حکومت اکثریت: در این سیستم‌های اجتماعی قدرت در دست اکثریت است. اگر اکثریت به خواسته‌ای اجتماعی مایل باشد آن خواسته برآورده می‌شود و اگر به خواسته‌ای اجتماعی مایل نباشد آن خواسته هیچ‌گاه برآورده نخواهد شد. یک ائتلاف اجتماعی (یک خواسته اجتماعی) برنده است اگر و تنها اگر اکثریت باشد.

نکته. در هر سه سیستم بالا در هر زمان تنها یک ائتلاف برنده می‌تواند وجود داشته باشد.

حکومت توزیع شده: در این سیستم‌های اجتماعی قدرت توزیع شده است، به این ترتیب که می‌تواند تعداد ائتلاف‌های اجتماعی برنده بیشتر از یک باشد به شرط آنکه خواسته این ائتلاف‌ها با هم در تضاد نباشند. اگر خواسته‌های اجتماعی $d_1, d_2, \dots, d_k$ با هم در تضاد نباشند همه آنها برنده و قابل انجام در سیستم اجتماعی هستند و اگر بین دو خواسته اجتماعی d_1, d_2 تضاد باشد آنگاه خواسته برنده خواسته اکثریت است. در این سیستم‌ها حقوق خصوصی و حقوق اقلیت لحاظ می‌شود.

۵-۵ منطقی برای ترجیحات^{۸۹}

چرا منطق بازی؟ با وجود نظریه بازی‌ها، روشهای منطقی چه کمکی می‌توانند بکنند؟

زبان منطق یک زبان صوری است و برای برنامه‌نویسی کامپیوتری اساسی است. منطق این امکان را به ما می‌دهد که به روش‌های اتوماتیک به درستیابی پروتکل‌هایی (استراتژی‌هایی) که برای اهداف خاص طراحی کرده‌ایم پردازیم و ببینیم آیا ویژگی‌های مورد نظر بعد از انجام پروتکل برآورده می‌شوند. برای مثال، مساله ۲-۳-۱، بریدن کیک، را در نظر بگیرید. چگونه ثابت کنیم که پروتکل حسادت آزاد درست کار می‌کند؟ چگونه ثابت کنیم که اگر در این پروتکل دو عامل با هم ائتلاف کنند باز هم بازیکن دیگر به هیچکدام حسادت نمی‌کند؟ برای اثبات و درستیابی کردن پروتکل‌ها اقتصادی، روش‌های نظریه بازی‌ها کارا نیست (روش‌های نظریه بازی‌ها چون حذف با تکرار استراتژی‌های مغلوب، روش بهترین پاسخ، روش استقرای وارون، و ... به دنبال پیدا کردن تعادل نش هستند).

در این بخش به مطالعه منطق ترجیحات می‌پردازیم. در یک بازی، عامل‌ها با توجه به ترجیحات خود و آگاهی که از ترجیحات عامل‌های دیگر دارند تصمیم‌گیری می‌کنند. منطق ترجیحات [؟،؟،؟] تلاش می‌کند^{۹۰} تا استدلال کند که

چگونه آگاهی یک عامل از ترجیحات عامل‌ها دیگر در تصمیم‌گیری او تاثیر می‌گذارد.

برای مثال، فرض کنید که می‌خواهید یک کیک را بین خود و دوستان تقسیم کنید. این که شما بدانید که دوستان از قسمت خامه‌ای کیک خوشش می‌آید تا اینکه این موضوع را ندانید، در نحوه تقسیم تاثیر می‌گذارد.

تعریف ۵-۵-۱. (مدل منطقی یک بازی). فرض کنید P یک مجموعه از گزاره‌های اتمی باشد. یک

مدل منطقی بازی عبارت است از چندتایی

$$M = \langle \Sigma, N, (A_i)_{i \in \Sigma}, P, \varepsilon, \rightarrow, (\leq_i)_{i \in \Sigma}, \pi, (\sim_i)_{i \in \Sigma}, n_0 \rangle$$

بطوریکه

۱. Σ یک مجموعه از بازیکن‌ها (عاملها) است.

۲. N مجموعه گره‌های گراف درختی است. (هر گره یا یک گره تصمیم‌گیری است که یک

بازیکن حق تصمیم‌گیری در آن دارد یا گره پایانی است)

۳. A_i یک مجموعه از عمل‌ها برای عامل i است.

۴. $\varepsilon : N - \text{Terminal}(N) \rightarrow \Sigma$ مشخص می‌کند که هر گره تصمیم‌گیری به کدام

بازیکن تعلق دارد. مجموعه $\text{Terminal}(N)$ برگها درخت است که در آن هیچ بازیکنی

تصمیم‌گیری نمی‌کند

۵. $\rightarrow : N \times \bigcup_{i \in P} A_i \rightarrow N$ یک تابع جزئی است که یالهای برجسب‌دار گراف را مشخص

می‌کند که باید خاصیت درخت بودن را حفظ کند. همچنین اگر $(n, a, m) \in \rightarrow$ آنگاه

$a \in A_{\varepsilon(n)}$ نماد $(n, a, m) \in \rightarrow$ را به صورت $n \xrightarrow{a} m$ نیز نمایش می‌دهیم.

۶. $\pi : \text{Termianl}(N) \rightarrow 2^P$ تابعی است که مشخص می کند در هر گره پایانی چه گزاره های اتمی ارضا می شود.

۷. $\leq_i \subseteq \text{Termianl}(N) \times \text{Terminal}(N)$ یک رابطه ترجیحات روی گره های پایانی است و $n \leq_i n'$ یعنی عامل i گره پایانی n' را به گره پایانی n ترجیح می دهد.

۸. $\sim_i \subseteq N \times N$ یک رابطه هم ارزی است بطوریکه اگر $n \sim_i m$ آنگاه $\varepsilon(n) = \varepsilon(m) = i$ رابطه $\sim_i$ مجموعه ای از گره ها را مشخص می کند که عامل i در هنگام انجام بازی مردد است که در کدام گره قرار دارد.

۹. اگر $n, m \in \varepsilon^{-1}(i)$ و $n \sim_i m$ آنگاه برای هر $a \in A_i$ ، یالی با برچسب a از گره n خارج می شود اگر و تنها اگر یالی با برچسب a از گره m خارج شود.

۱۰. n_0 گره آغازین بازی.

(این تعریف را با تعریف درخت بازی ۵-۲-۱ مقایسه کنید. تابع سود ν حذف شده است و به جای آن روابط ترجیحات $\leq_i$ و تابع ارزش π اضافه شده است.)

نمادگذاری. در یک مدل بازی، تابع تالی $Succ : N \rightarrow 2^N$ را بصورت

$$Succ(n) = \{n' \in N \mid \exists a \in A_{\varepsilon(n)} (n \xrightarrow{a} n')\}$$

در نظر می گیریم.

تعریف ۵-۵-۲. در مدل منطقی بازی M .

○ عامل i مجموعه $S \subseteq \text{Terminal}(N)$ را ترجیح می‌دهد هرگاه

$$(\forall n \in S)(\forall n' \in \text{Terminal}(N) - S)(n' \leq_i n)$$

○ یک ائتلاف $\Gamma \subseteq \Sigma$ از عاملها مجموعه $S \subseteq \text{Terminal}(N)$ را ترجیح می‌دهد هرگاه هر

عامل $i \in \Gamma$ مجموعه S را ترجیح دهد.

○ یک استراتژی S_Γ برای یک ائتلاف Γ ، یک مجموعه از استراتژی‌های اعضای Γ است. برای

گره $n \in N$ ، اگر این گره، گره تصمیم‌گیری یکی از اعضای ائتلاف Γ باشد، $\varepsilon(n) \in \Gamma$ ،

آنگاه $S_\Gamma(n) := \{s_{\varepsilon(n)}(n) \mid s_{\varepsilon(n)} \in S_\Gamma\}$ تعریف می‌شود.

○ برای دو استراتژی S_Γ^1 و S_Γ^2 می‌نویسیم $S_\Gamma^1 \subseteq S_\Gamma^2$ هرگاه برای هر $n \in N$ اگر

$$S_\Gamma^1(n) \subseteq S_\Gamma^2(n) \quad \varepsilon(n) \in \Gamma$$

تعریف ۵-۵-۳. (به روز رسانی مدل بازی)

• یک مسیر اجرا از یک مدل بازی عبارت است از مسیر $n_0, n_1, \dots, n_z$ روی درخت درخت

بازی که از ریشه n_0 آغاز می‌شود و برای هر k ، $n_{k+1} \in \text{succ}(n_k)$ و گره پایانی n_z گره پایانی است.

• گوییم مسیر اجرا $n_0, n_1, \dots, n_z$ با S_Γ ، استراتژی ائتلاف Γ ، سازگار است هرگاه برای هر

$$(n_k, n_{k+1}) \text{ که } \varepsilon(n_k) \in \Gamma \text{ داشته باشیم } n_{k+1} \in S_\Gamma(n_k)$$

• به روز رسانی مدل بازی

$$M = \langle \Sigma, N, (A_i)_{i \in \Sigma}, P, \varepsilon, \rightarrow, (\leq_i)_{i \in \Sigma}, \pi, (\sim_i)_{i \in \Sigma}, n_0 \rangle$$

توسط استراتژی S_Γ ، مدل بازی

$$\text{update}(M, S_\Gamma) = \langle \Sigma, N', (A_i)_{i \in \Sigma}, P, \varepsilon, \rightarrow', (\leq'_i)_{i \in \Sigma}, \pi', (\sim'_i)_{i \in \Sigma}, n_0 \rangle$$

است که تشکیل می‌شود از همه **مسیرهای اجرایی** از درخت مدل M که با S_Γ سازگار است.

یعنی، مجموعه N' عبارت است از گره‌هایی که با شروع از ریشه و رابطه

$$\rightarrow' = \left\{ (n, a, n') \in \rightarrow \mid (\varepsilon(n) \in \Gamma \Rightarrow a \in S_\Gamma(n)) \right\}$$

بدست می‌آید. $(\leq'_i)_{i \in \Sigma}, \pi', (\sim'_i)_{i \in \Sigma}$ از تحدید روابط $(\leq_i)_{i \in \Sigma}, \pi, (\sim_i)_{i \in \Sigma}$ به گره‌های

درخت مدل جدید بدست می‌آید.

توجه کنید که در مدل به روز رسانی شده $\text{update}(M, S_\Gamma)$ تنها عامل‌های ائتلاف Γ محدود

به پیروی از استراتژی S_Γ هستند و عامل‌های دیگری می‌توانند هر استراتژی را انجام دهند.

گرامر منطق ترجیحات

فرض کنید P یک مجموعه از گزاره‌های اتمی باشد. زبان PL (زبان گزاره‌ای روی P) را

کوچکترین مجموعه‌ای شامل P بپذیرید بطوریکه

$$\psi, \varphi \in PL \Rightarrow \neg\psi, (\psi \vee \varphi) \in PL.$$

تعریف ۵-۵-۴. برای مجموعه P از گزاره‌های اتمی، و مجموعه Σ از عامل‌ها زبان منطق

ترجیحات L کوچکترین مجموعه‌ای است که

$$\psi_0 \in PL \text{ and } \psi, \varphi \in L \Rightarrow \neg\psi, (\psi \vee \varphi), \Box\psi_0, [\Gamma : \psi_0]\varphi \in L$$

$\Box\psi_0$ این معنا را می‌دهد که در هر خروجی نهایی بازی گزاره ψ_0 درست است.

$[\Gamma : \psi_0]\varphi$ این معنا را می‌دهد که در بازی که ائتلاف Γ گزاره ψ_0 را ترجیح دهند گزاره φ

اتفاق خواهد افتاد

معناشناسی

مدل منطقی بازی

$$M = \langle \Sigma, N, (A_i)_{i \in \Sigma}, P, \varepsilon, \rightarrow, (\leq_i)_{i \in \Sigma}, \pi, (\sim_i)_{i \in \Sigma}, n_0 \rangle$$

را در نظر بگیرید. برای گره‌های پایانی، $s \in \text{Terminal}(N)$ ، و فرمول‌های زبان گزاره‌ای PL ،

ارضا شدن را بصورت زیر تعریف می‌کنیم.

$$\pi, s \models p \quad \text{iff} \quad p \in \pi(s)$$

$$\pi, s \models \varphi \vee \psi \quad \text{iff} \quad \pi, s \models \varphi \text{ or } \pi, s \models \psi$$

$$\pi, s \models \neg\varphi \quad \text{iff} \quad \text{not } \pi, s \models \varphi$$

تعریف ۵-۵-۵. برای فرمول‌های زبان منطق ترجیحات، L ، و مدل بازی M ، ارضا شدن بصورت زیر

تعریف می‌شود.

$$M \models \Box \psi_0 \text{ iff } \forall s \in \text{Terminal}(N) \pi, s \models \psi_0$$

$$M \models \varphi \vee \psi \text{ iff } M \models \varphi \text{ or } M \models \psi$$

$$M \models \neg \varphi \text{ iff } \text{not } M \models \varphi$$

$$M \models [\Gamma : \psi_0] \varphi \text{ iff } Up(M, \Gamma, \psi_0) \models \varphi$$

$Up(M, \Gamma, \psi_0)$ به روز رسانی مدل بازی M با توجه به ترجیح ψ_0 توسط ائتلاف Γ است، که

در آن ائتلاف Γ طوری عمل می کند تا گزاره ψ_0 را در پایان تضمین کند.

$Up(M, \Gamma, \psi_0)$ به صورت زیر تعریف می شود.

برای فرمول گزاره ای ψ_0 گوئیم ائتلاف Γ ، در مدل بازی M ، گزاره ψ_0 را ترجیح می دهد هرگاه

ائتلاف Γ مجموعه $S = \{s \mid \pi, s \models \psi_0\}$ را ترجیح دهد.

تعریف ۵-۵-۶

گوئیم استراتژی S_Γ گزاره φ_0 را در مدل بازی M **تضمین** می کند هرگاه برای هر گره

پایانی s از قاب بازی $update(M, S_\Gamma)$ داشته باشیم $\pi, s \models \varphi_0$.

گوئیم ائتلاف Γ می تواند گزاره φ_0 را در مدل بازی M تضمین کند هرگاه استراتژی

S_Γ موجود باشد که φ_0 را تضمین کند.

گوئیم استراتژی S_Γ گزاره φ_0 را در مدل بازی M **بطور کامل تضمین** می کند هرگاه

برای هر زیربازی^{۹۱} M' از M ، اگر ائتلاف Γ بتواند گزاره φ_0 را در زیربازی M'

تضمین کند آنگاه (همان) S_Γ گزاره φ_0 را در زیربازی M' نیز تضمین کند.

^{۹۱} تعریف زیربازی در بخش بازی های دینامیک را ببینید.

تعریف ۵-۵-۷ گیرید $S_{\Gamma}^*(M, \varphi_0)$ کلی ترین استراتژی برای ائتلاف Γ باشد که گزاره φ_0 را در مدل بازی M بطور کامل تضمین می کند (یعنی استراتژی چون S_{Γ} که گزاره φ_0 را در مدل بازی F بطور کامل تضمین کند وجود نداشته باشد که $S_{\Gamma}^* \subset S_{\Gamma}$). تعریف می کنیم

$$Up(M, \Gamma, \varphi_0) = \langle \text{update}(M, S_{\Gamma}^*(M, \varphi_0)) \rangle$$

مثال ۵-۵-۴ (پروتکل رای گیری)

سه عامل A, B, C باید (دقیقا) یکی از سه گزینه x, y, z را انتخاب کنند. یک پروتکل رای گیری برای عاملها باید دو ویژگی زیر را داشته باشد که

الف: بعد از اجرای پروتکل یک و تنها گزینه انتخاب شده باشد، و

ب: گزینه بیرون آمده از پروتکل، نظر اکثریت باشد.

این ویژگی ها را به کمک منطق ترجیحات بصورت زیر می توان توصیف کرد. بگذارید

$$\Gamma \subseteq \{A, B, C\} \text{ و گزاره های اتمی } P = \{x, y, z\} \text{ باشد.}$$

شرایط نهایی مورد نظر:

$$\bigcirc \text{ در پایان یک گزینه انتخاب می شود: } \Box(x \vee y \vee z)$$

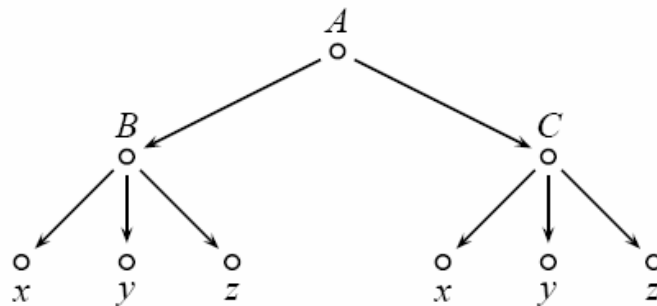
$$\bigcirc \text{ در پایان حداکثر یک گزینه انتخاب می شود: } \bigwedge_{u, v \in P, u \neq v} \Box \neg(u \wedge v)$$

$$\bigcirc \text{ نظر اکثریت اتفاق می افتد: برای هر } |\Gamma| > 1, \Box_{u \in P} [\Gamma : u] \Box u$$

بعد از اجرای هر پروتکل رای‌گیری مناسب باید شرایط فوق را ارضا شود. مثلاً این پروتکل که از عامل‌ها بخواهیم روی یک کاغذ گزینه مورد نظر خود را بنویسند و هر گزینه که بیشتر رای آورد انتخاب شود، شرایط نهایی فوق را برآورده نمی‌کند. **زیرا ممکن است هر سه عامل به سه گزینه متفاوت رای دهند.**

در زیر دو پروتکل رای‌گیری متمایز را در نظر می‌گیریم.

پروتکل Pr1: عامل A یکی از دو عامل دیگر B, C را انتخاب می‌کند و به او برای رای خود وکالت می‌دهد، یعنی عامل انتخاب شده توسط A هر گزینه‌ای را انتخاب کند عامل A نیز همان گزینه را انتخاب کرده است. مسلماً عامل A باید از ترجیحات عامل‌های B, C آگاه باشد تا بتواند با توجه به ترجیحات خود یکی از آن‌ها را وکیل خود کند. شکل زیر را ببینید^{۹۲}



داریم: $\text{Pr1} \models [AB : x] \Box x$ و $\text{Pr1} \models [B : x][A : x] \Box x$.

اما $\text{Pr1} \not\models [A : x][B : x] \Box x$ چرا؟

آیا این پروتکل شرایط نهایی را برآورده می‌کند؟ (بله)

^{۹۲} شکل از منبع [۴] بر داشته شده است.

پروتکل Pr2: پروتکل دیگری برای رای گیری که شرایط نهایی مساله را برآورده سازد می توان در نظر

گرفت. به این ترتیب که، ابتدا عامل A به یکی از سه گزینه رای می دهد، سپس عامل B به یکی از سه گزینه رای می دهد. اگر دو عامل A, B به گزینه یکسانی رای داده باشند آن گزینه انتخاب جمع خواهد بود، وگرنه، عامل C به یکی از دو گزینه ای که A و B رای داده اند رای می دهد (عامل C تنها دو گزینه برای رای دادن در پیش رو دارد)، و هر گزینه ای که عامل C به آن رای دهد انتخاب خواهد شد.

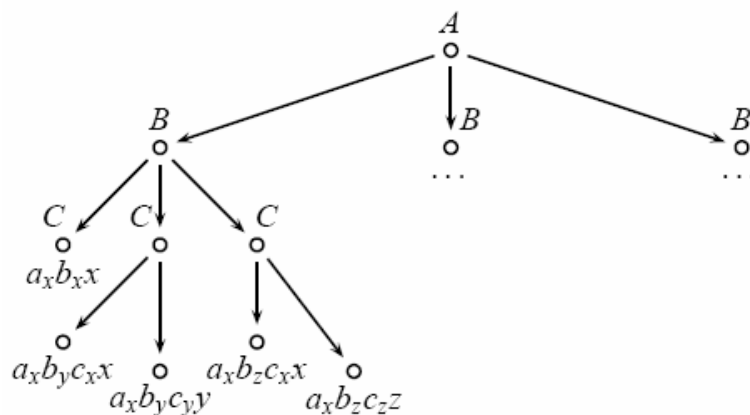
مجموعه گزاره های اتمی $P' = P \cup \{a_e, b_e, c_e \mid e \in \{x, y, z\}\}$ را در نظر می گیریم که

a_e یعنی عامل A به گزینه e رای داده است،

b_e یعنی عامل B به گزینه e رای داده است، و

c_e یعنی عامل C به گزینه e رای داده است.

در شکل پروتکل Pr2 نمایش داده شده است و این که چه گزاره های اتمی در گره های نهایی ارضا می شوند.



پروتکل Pr2 نیز شرایط نهایی مورد نظر ما را ارضا می کند (چرا؟)

در پروتکل Pr2 عامل A آزاد است که به هر گزینه ای (مثلا x) رای بدهد. اما عامل C برای رای دادن خود آزاد نیست و اینطور نیست که اگر او بخواهد به x رای بدهد حتمی بتواند.

$$\text{Pr2} \models [A : a_x] \Box a_x$$

$$\text{Pr2} \not\models [C : c_x] \Box c_x$$

همچنین اگر عامل C در پروتکل رای بدهد رای او همیشه تعیین کننده انتخاب نهایی خواهد بود، در حالی که برای عامل A اینگونه نیست.

$$\text{Pr2} \models \Box ((c_x \rightarrow x) \wedge (c_y \rightarrow y) \wedge (c_z \rightarrow z))$$

$$\text{Pr2} \not\models \Box ((a_x \rightarrow x) \wedge (a_y \rightarrow y) \wedge (a_z \rightarrow z))$$

در پروتکل Pr2 همواره برای عامل C عقلانی است که (از بین گزینه هایی که می تواند به آنها رای دهد) اگر گزینه ای را ترجیح نمی دهد به آن رای ندهد

$$\text{Pr} \models [C : \neg x] \Box \neg c_x$$

در حالی که برای عامل A اینگونه نیست. اگر عامل A گزینه x را ترجیح دهد ولی بداند که عامل B و C هر دو گزینه y را ترجیح می دهند آنگاه این عقلانی نیست که A به x رای بدهد. فرض کنید که ترجیحات عامل ها بصورت زیر باشد.

$$x >_A y >_A z$$

$$z >_B x >_B y$$

$$y >_C x >_C z$$

باتوجه به ترجیحات فوق

۱. عامل A فرمولهای $x, x \vee y$ را ترجیح می‌دهد،

۲. عامل B فرمولهای $z, x \vee z$ را ترجیح می‌دهد،

۳. عامل C فرمولهای $y, x \vee y$ را ترجیح می‌دهد، و

۴. ائتلاف AC فرمول $x \vee y$ را ترجیح می‌دهد.

می‌توان دید برای پروتکل Pr1 با ترجیحات داده شده، انتخاب نهایی y است، که ارضا شدن این موضوع را تایید می‌کند.

$$\text{Pr1} \models [A : x][C : y][AC : x \vee y] \Box y$$

عامل A با توجه به آگاهی که از ترجیحات دو عامل دیگر دارد، به عامل C وکالت می‌دهد. دقت کنید که آگاهی عامل‌ها از ترجیحات یکدیگر اساسی است.

همچنین برای پروتکل Pr2 داریم:

$$\text{Pr2} \models [A : x][C : y][AC : x \vee y] \Box y$$

$$\text{Pr2} \models [B : x \vee z][C : x \vee y][A : x] \Box x$$

۵-۶ مدل سازی

در این قسمت، می خواهیم به کمک منطق ترجیحات به مدل سازی منطقی پروتکل تقسیم حسادت آزاد کیک (مساله ۲-۳-۱) بپردازیم. همانند منطق شناختی که به منظور مدل سازی، مدل کریپکی سیستم چندعاملی، گزاره های اتمی و عمل های شناختی پروتکل مساله را مشخص می کردیم، در اینجا نیز مدل منطقی بازی، گزاره های اتمی و استراتژی های پروتکل را برای مدل سازی مشخص می کنیم.

مدل سازی تقسیم حسادت آزاد آش شعله قلمکار



الان که دارم این بخش را می نویسم، هوا سرد است و آش را به کیک ترجیح می دهم

آذر a ، باران b ، و کیهان c یک دیگ آش (Y) پخته اند.



دیگ آش Y

آنها می خواهند این آش را به طور حسادت آزاد بین خود تقسیم کنند. برای این کار یازده کاسه خالی



X_1, X_2, X_3, V و E, E_1, E_2, E_3 و A, B, C با گنجایش نامحدود در اختیار دارند.

هشت کاسه X_1, X_2, X_3, V و E, E_1, E_2, E_3 برای اجرا پروتکل استفاده می‌شوند و کاسه‌های

A, B, C ، کاسه‌هایی شخصی خواهند بود که به ترتیب کیهان، باران و آذر در نهایت سهم آتش خود در

آنها خواهند داشت. ابتدا مدل منطقی بازی را ارائه می‌دهیم:

مدل منطقی بازی:

برای مشخص کردن مدل منطقی بازی

$$M = \langle \Sigma, N, (A_i)_{i \in \Sigma}, P, \varepsilon, \rightarrow, (\leq_i)_{i \in \Sigma}, \pi, (\sim_i)_{i \in \Sigma}, n_0 \rangle$$

باید چندتایی بالا را تعریف کنیم. مجموعه $\Sigma = \{a, b, c\}$ خواهد بود.

ابتدا درخت بازی

$$\langle N, \varepsilon, \rightarrow, (\sim_i)_{i \in \Sigma}, n_0 \rangle$$

N مجموعه گره‌ها، ε تابع مشخص کننده تصمیم‌گیرنده گره‌ها، $\rightarrow$ یالها، $(\sim_i)_{i \in \Sigma}$ رابطه مردد

بودن، را در زیر شرح می‌دهیم.

در گام اول، آذر آتش داخل دیگ Y را به سه کاسه X_1, X_2, X_3 منتقل می‌کند. آذر با توجه به

ترجیحاتش می‌تواند عمل‌هایی مانند زیر را انجام دهد:

۱. کاسه‌ها را طوری پر کند که کاسه X_1 را به X_2, X_3 ترجیح دهد ولی X_2, X_3 از لحاظ او

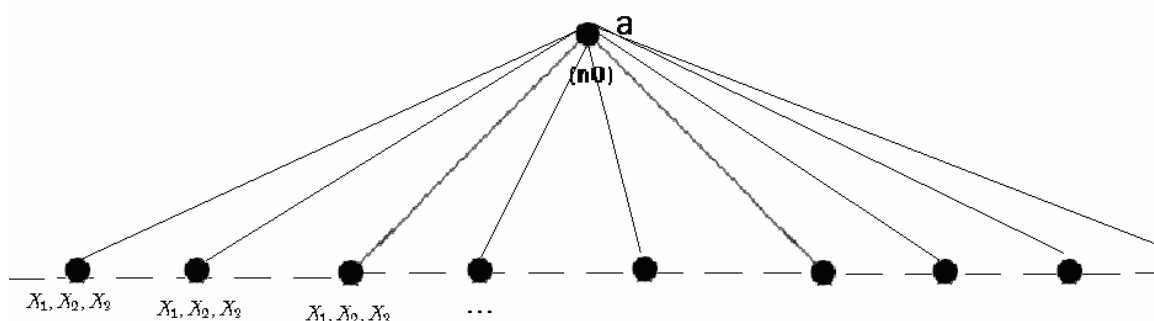
یکسان باشند

۲. کاسه‌ها را طوری پر کند که هر سه کاسه از لحاظ او یکسان باشند

۳. ...

با توجه به اینکه چگونه آذر a ، آش را از دیگ به سه کاسه X_1, X_2, X_3 منتقل کند

$1 + 2 \binom{3}{2} + 3!$ حالت ممکن برای اینکه آذر چگونه کاسه‌ها را به هم ترجیح می‌دهد اتفاق می‌افتد.



تصویر ۱

تعداد برگ‌های درخت تصویر بالا $1 + 2 \binom{3}{2} + 3!$ است (از گره آغازین $1 + 2 \binom{3}{2} + 3!$ یال

خارج می‌شود). هر برگ درخت تصویر ۱، یک گره تصمیم‌گیری برای باران b است. از آنجا که باران از

ترجیحات آذر a آگاه نیست، بین این گره‌ها خط چین گذاشته شده است.

در گام دوم، باران دو کاسه از سه کاسه X_1, X_2, X_3 را برمی‌دارد (مثلاً $[X_1, X_2]$) و آش یکی از

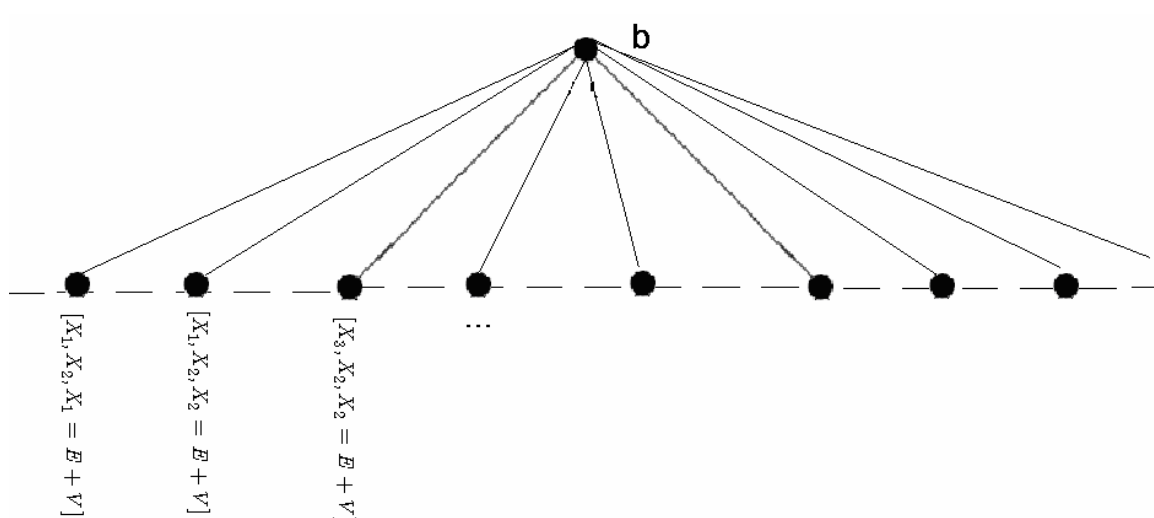
این دو کاسه را (مثلاً X_2) در دو کاسه جدید V و E می‌ریزد.

باران می‌تواند $\binom{3}{2}$ حالت دو کاسه را به سمت خود بکشد و از بین دو کاسه انتخابی $\binom{2}{1}$ یک کاسه را

در V و E خالی کند. با توجه به رابطه ترجیحات باران بین ۴ کاسه پر،

$$\binom{3}{2}\binom{2}{1}\left(1+2\binom{4}{3}+2\binom{4}{2}+3!\binom{4}{2}+4!\right)$$

حالت ممکن بعد از عمل باران بوجود می‌آید. از آنجا که باران بین همه گره‌های درخت تصویر ۱ مردد بود، از هر برگ تصویر ۱ درخت تصویر ۲ ادامه می‌یابد.



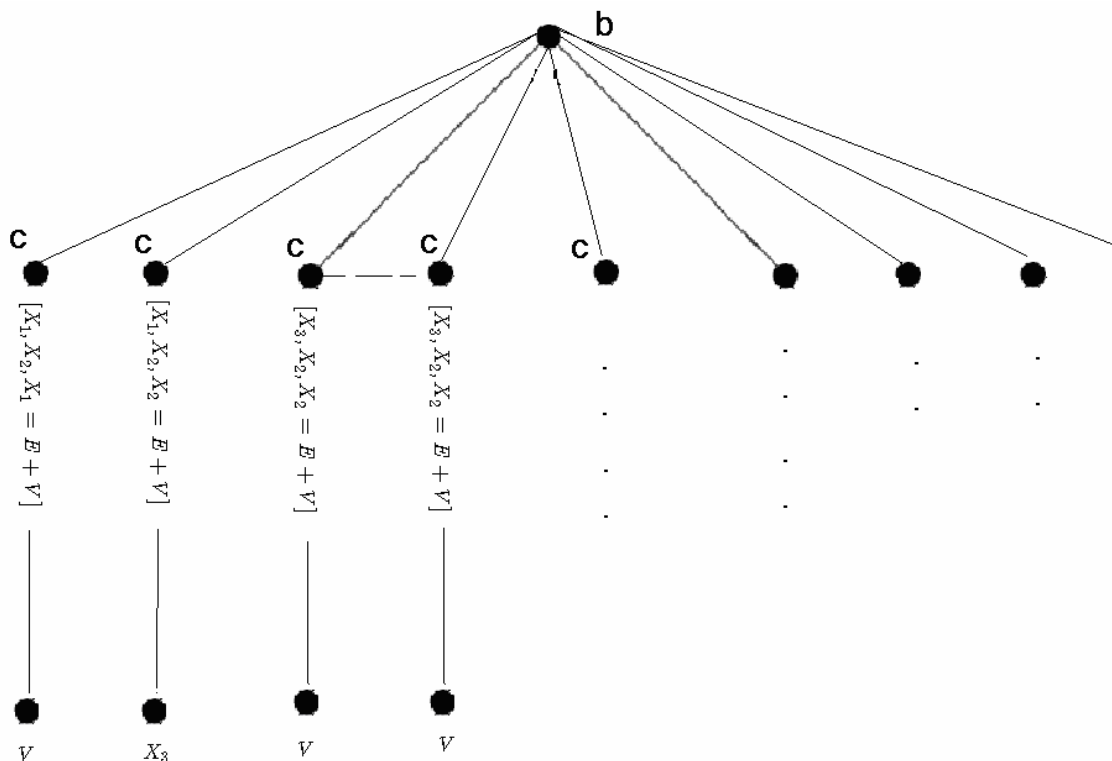
تصویر ۲

درخت تصویر ۲، $\left(\binom{3}{2}\binom{2}{1}\left(1+2\binom{4}{3}+2\binom{4}{2}+3!\binom{4}{2}+4!\right)\right)$ برگ دارد که هر برگ این

درخت یک گره تصمیم‌گیری برای کیهان c است. از آنجا که کیهان از ترجیحات باران خبر ندارد اگر در دو برگ متمایز تصویر ۲، دو کاسه انتخاب شده یکسان باشند و کاسه‌ای که در E و V نیز خالی شده است یکسان باشد آنگاه کیهان نمی‌تواند این دو حالت ممکن را از هم تمییز دهد.

در گام سوم، کیهان از بین چهار کاسه پر، یک کاسه به غیر از کاسه E را انتخاب می‌کند و آن را در

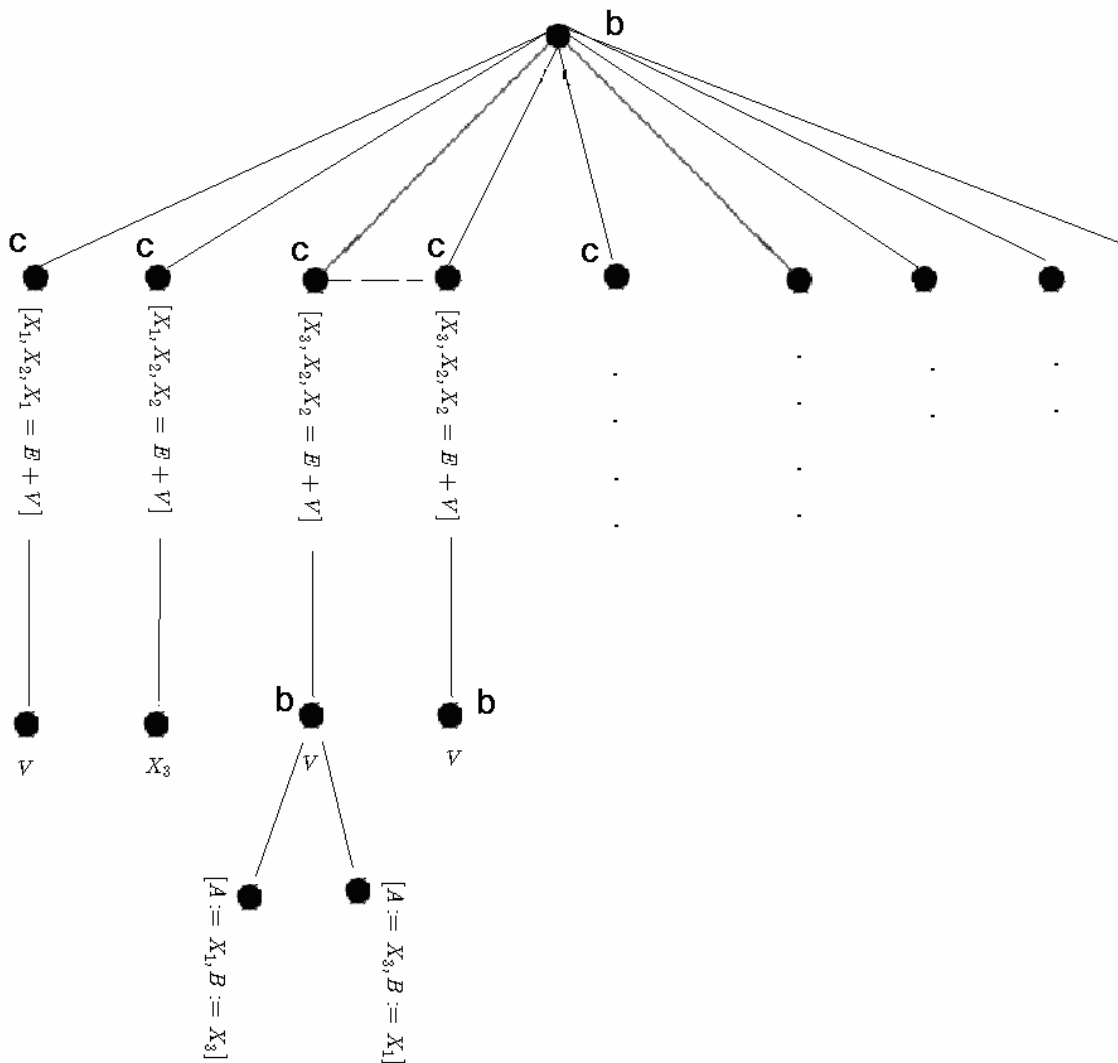
کاسه شخصی C خود می‌ریزد. دقت کنید که اگر در تصویر درخت ۲، دو گره را کیهان نتواند از هم تمییز دهد باید در هر دو گره کاسه یکسانی را به کاسه شخصی خود خالی کند.



تصویر ۳

در گام چهارم، اگر کیهان کاسه V را بردارد آتش کاسه V در کاسه شخصی B باران ریخته می‌شود و آتش کاسه پر دیگر (به غیر از کاسه E) در کاسه شخصی A آذر ریخته می‌شود.

اگر کیهان کاسه V را بردارد، برگهای درخت تصویر ۳ که در آن کیهان V را انتخاب کرده است، گره تصمیم‌گیری باران خواهد بود که او از بین دو کاسه آتش پر (به غیر از کاسه E) یک کاسه را در کاسه شخصی خود B و کاسه دیگر را در کاسه شخصی آذر A می‌ریزد.



تصویر ۴

در هر گره پایانی درخت تصویر ۴، از بین باران و کیهان، آن کسی که کاسه V را انتخاب نکرده است،

گره پایانی به عنوان گره تصمیم‌گیری در اختیار اوست. برای هر گره پایانی درخت تصویر ۴، کسی که

تصمیم‌گیرنده در این گره است آتش کاسه E را در کاسه‌های E_1, E_2, E_3 می‌ریزد با توجه به

ترجیحات عامل $3! + 2 \binom{3}{2} + 1$ حالت ممکن می‌تواند اتفاق بیفتد (یعنی از این گره تصمیم‌گیری

$3! + 2 \binom{3}{2} + 1$ یال خارج می‌شود).

سپس در برگهای جدیدی که بوجود می‌آید، اگر در پایین‌ترین پدر برگ، تصمیم‌گیرنده کیهان باشد در این برگ، تصمیم‌گیرنده باران است و اگر باران باشد تصمیم‌گیرنده کیهان است. تصمیم‌گیرنده یکی از کاسه‌های E_1, E_2, E_3 را در کاسه شخصی خود می‌ریزد، که سه حالت ممکن است (یعنی از این برگ ۳ یال خارج می‌شود). سپس در هر برگ جدید، آذر تصمیم‌گیرنده خواهد بود که او نیز یک کاسه از کاسه‌ها پر باقیمانده از E_1, E_2, E_3 را در ظرف شخصی خود و کاسه دیگر را در کاسه شخصی کسی می‌ریزد که در پایین‌ترین پدر برگ تصمیم‌گیرنده نبوده است (از این برگ دو یال خارج می‌شود).

به این ترتیب، درخت بازی را شرح دادیم.

رابطه‌ها ترجیحات $\leq_a, \leq_b, \leq_c$ به صورت زیر روی گره‌های پایانی درخت بصورت زیر تعریف می‌شود که برای مثال آذر یک گره پایانی را به گره پایانی دیگر ترجیح می‌دهد هرگاه کاسه شخصی خود را در گره اول به کاسه شخصی‌اش در گره دوم ترجیح دهد. فقط رابطه ترجیحات هر عامل باید با ترجیحاتش در مورد آش کاسه‌های دیگر X_1, X_2, X_3, V و E, E_1, E_2, E_3 در گره‌های میانی سازگار باشد.

مجموعه گزاره‌های اتمی P بصورت زیر تعریف می‌شود.

$$P = \{q_{i,x,y} \mid i \in \{a, b, c\}, x, y \in \{X_1, X_2, X_3, V, E, E_1, E_2, E_3, A, B, C\}\}$$

$q_{i,x,y}$ این معنا را می‌دهد که عامل i کاسه x را به اندازه کاسه y ترجیح می‌دهد. گزاره‌های اتمی چگونه در گره‌های پایانی ارضا می‌شوند؟ برای مشخص کردن تابع π ، ارزش گزاره‌های اتمی، به مسیری که از ریشه به این گره رسیدیم نگاه می‌کنیم.

بگذارید، در ادامه، برای راحتی از نماد $e_{i,x,y}$ برای فرمول مرکب $q_{i,x,y} \wedge q_{i,y,x}$ استفاده کنیم.

اکنون می‌توانیم گزاره‌هایی را در مورد مساله بنویسیم و با روش بررسی گر مدل درست‌یابی کنیم.

برای مثال،

$$[\{a\} : (e_{a,x_1,x_2} \wedge e_{a,x_2,x_3})](q_{a,A,B} \wedge q_{a,A,C})$$

یعنی اگر عامل a از بین $1 + 2 \binom{3}{2} + 3!$ تقسیم آتش دیگر در ظرف‌های X_1, X_2, X_3

استراتژی‌اش این باشد طوری آتش را در این ۳ کاسه تقسیم کند که همه ظرف‌ها ارجحیت یکسانی برای او داشته باشند، آنگاه در پایان انجام پروتکل، سهم آتش خود را به دو نفر دیگر ترجیح می‌دهد.

تمرین. جمله‌ها دیگری نیز در مورد پروتکل بیان کنید، آنها را به زبان منطق ترجیحات توصیف کنید، و به روش بررسی گر مدل درست‌یابی کنید.

تمرین. جمله‌ای را در مورد پروتکل بیان کنید که نتوان آن را به کمک گزاره‌ها اتمی مجموعه P توصیف کرد. گزاره‌های اتمی جدیدی به مجموعه P اضافه کنید (برای اینکار نیاز دارید کاسه‌های جدیدی استفاده کنید که آتش قبل از منتقل شدن به کاسه‌های شخصی به آنها منتقل شود تا بعضی مقادیر را بتوانید در متغیر آن کاسه ذخیره کنید) و جمله را به زبان منطق ترجیحات توصیف کنید.

تمرین

۱. تمرین‌های داخل فصل را حل کنید.
۲. پروتکل تقسیم عادلانه کیک را مدل‌سازی منطقی کنید.

مراجع

1. J.N. Webb, **Game Theory, Decisions, Interaction, and Evolution**, 2007
2. B. Peleg, P. Sudholter, **Introduction to the theory of cooperative games**, 2007
3. R. Gibbons, **A primer in Game Theory**
4. N. Nisan, T. Roughgarden, E. Tardos, V.V. Vazirani (Editors), **Algorithmic Game theory**, 2007 (specially, see the part II, Algorithmic Mechanism Design)
5. N. McCarty, A. Meirowitz, **Political Game Theory, an introduction**, 2007.
6. M. Pauly, **Logic for Social Software**, PhD Thesis, ILLC, 2001.
7. S. van Otterloo, **A Strategic Analysis of Multi-agent Protocols**, PhD Thesis, ILLC, 2005.

منطق تکلیف

منطق تکلیف، منطقی است که می‌تواند مورد استفاده فقیهان مذاهب، وکیل‌ها و قاضی‌ها قرار گیرد. این

منطق با موجهاتی چون

مجاز است که

واجب (متعهد) است که ...

حرام (ممنوع) است که ...

محق^{۹۳} است که ...

سر کار دارد. یک عامل در یک اجتماع توسط یک مجموعه از قوانین مورد داوری قرار می‌گیرد. این که عامل با توجه به قوانین، مجاز به انجام چه کارهایی است، چه کارهایی را نباید و چه کارهایی را باید انجام دهد، و از چه حقوق انسانی-اجتماعی برخوردار است را باید بتوان از قوانین وضع شده استنتاج کرد. در این فصل، به معرفی منطق تکلیف خواهیم پرداخت.

(این فصل کامل نیست و با اهداف درس برای سیستم‌های اجتماعی فاصله زیادی دارد. باید منطق

تکلیف چندعاملی و تحت عمل (action-based) اضافه شود)

۶-۱ منطق تکلیف

زبان منطق تکلیف با اضافه کردن دو عملگر O و P به زبان منطق گزاره‌ای بدست می‌آید. فرض کنید

At مجموعه گزاره‌های اتمی سیستم اجتماعی باشد. $L^D(At)$ (زبان منطق تکلیف روی اتم‌های

At) کوچکترین مجموعه‌ای است که:

$$1. At \subseteq L^D(At)$$

$$2. \varphi, \psi \in L^D(At) \Rightarrow \varphi \wedge \psi, \neg\varphi, O\varphi, P\varphi \in L^D(At)$$

$O\varphi$ یعنی "واجب است φ محقق شود" یا یعنی "عامل به φ متعهد است".

$P\varphi$ یعنی "جایز است φ محقق شود".

در منطق تکلیف دو قاعده استنتاج زیر را در نظر می‌گیریم.

$$R1. \frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

$$R2. \frac{\varphi}{O\varphi}$$

اصول موضوع زیر را در نظر بگیرید.

۱. همانگویی‌های منطق گزاره‌ای

$$2. P\varphi \leftrightarrow \neg O\neg\varphi \quad (\varphi \text{ جایز است اگر و تنها اگر نقیض آن واجب نباشد})$$

$$3. O(\varphi \rightarrow \psi) \rightarrow (O\varphi \rightarrow O\psi)$$

$$4. O\varphi \rightarrow P\varphi$$

$$5. O\varphi \rightarrow OO\varphi$$

$$6. PO\varphi \rightarrow O\varphi$$

$$O(O\varphi \rightarrow \varphi) \quad ۷$$

$$O(PO\varphi \rightarrow \varphi) \quad ۸$$

دستگاه‌های استاندارد زیادی را می‌توان برای منطق تکلیف در نظر گرفت. در اینجا تنها دو دستگاه

$S5^+$ و OB^+ را معرفی می‌کنیم.

دو قاعده استنتاج $R1, R2$ همراه با اصول موضوعه ۱ تا ۶ دستگاه برهان $S5^+$ را تشکیل می‌دهند.

دو قاعده استنتاج $R1, R2$ همراه با اصول موضوعه ۱ تا ۴ و اصول ۷ و ۸ دستگاه برهان OB^+ را می-

سازند.

معناشناسی

یک مدل کریپکی برای منطق تکلیف روی مجموعه فرمولهای اتمی At عبارت است از سه‌تایی

$M = \langle S, R, V \rangle$ که S مجموعه حالت‌های ممکن، $R \subseteq S \times S$ رابطه دسترسی، و

$V : S \rightarrow 2^{At}$ تابعی است که مشخص می‌کند در هر حالت چه گزاره‌های اتمی صادق است.

برقراری گزاره‌های زبان $L^D(At)$ در مدل نقطه‌ای (M, s) بصورت زیر تعریف می‌شود.

$$(M, s) \models p \quad \text{iff} \quad p \in V(s)$$

$$(M, s) \models (\varphi \wedge \psi) \quad \text{iff} \quad (M, s) \models \varphi \text{ and } (M, s) \models \psi$$

$$(M, s) \models \neg\varphi \quad \text{iff} \quad \text{not}(M, s) \models \varphi$$

$$(M, s) \models O\varphi \quad \text{iff} \quad \text{for all } t \text{ such that } R(s, t), (M, t) \models \varphi$$

$$(M, s) \models P\varphi \quad \text{iff} \quad \text{there exists } t \text{ such that } R(s, t), (M, t) \models \varphi$$

یک مدل کریپکی $S5^+$ است هرگاه رابطه R سریال، اقلیدسی، و تراگذری باشد.

یک مدل کریپکی OB^+ است هرگاه رابطه R سریال، تقریباً متقارن^{۹۴}، و تقریباً بازتابی^{۹۵} باشد. می‌توان قضیه صحت و تمامیت را برای دستگاه برهان $S5^+$ و مدل‌های کریپکی $S5^+$ اثبات کرد، همچنین قضیه صحت و تمامیت برای دستگاه برهان OB^+ و مدل‌های کریپکی OB^+ نیز برقرار است.

۶-۲ تنازعه‌ها

با در نظر گرفتن اصول موضوعه ارائه شده در بالا تنازعه‌هایی در منطق تکلیف بوجود می‌آید که در زیر برای نمونه به چندتا از آنها اشاره می‌کنیم.

تنازع راس:

۱. تو باید نامه را پست کنی

۲. تو باید یا نامه را پست کنی یا آن را آتش بزنی

فرض کنید p : نامه را پست می‌کنی و q : نامه را آتش می‌زنی باشد. اگر بخواهیم دو گزاره بالا را به زبان منطق تکلیف بنویسیم داریم.

۱. Op

۲. $O(p \vee q)$

از طرفی $p \rightarrow (p \vee q)$ ، پس بنابر قاعده ۲ داریم $O(p \rightarrow (p \vee q))$ و از اصل ۳ بدست می‌آید

که $Op \rightarrow O(p \vee q)$!

^{۹۴} رابطه R تقریباً متقارن است هرگاه $\forall xyz(xRy \rightarrow (yRz \rightarrow zRy))$

^{۹۵} رابطه R تقریباً بازتابی است هرگاه $\forall xy(xRy \rightarrow yRy)$

تنازع ...

.....

۶-۳ سیستم‌های هنجاری^{۹۶}

(پیش‌نیاز این بخش جزوه، منطق زمانی در فصل آینده است. برای مطالعه به فصل بعدی مراجعه کنید.)

قانونگذاری را در نظر بگیرید که می‌خواهد برای یک سیستم اجتماعی قوانین و **هنجارهایی** را وضع کند.

قانونگذار باید بتواند نشان دهد که قوانینی که او وضع می‌کند **کارایی** سیستم را بالا می‌برد،

می‌توان قوانین را به دو نوع قوانین بازدارنده و قوانین تسهیل کننده تقسیم کرد.

قوانین بازدارنده: قوانینی هستند که از ترس اینکه در صورت رعایت نکردن آنها وضعیت بدی اتفاق افتد وضع می‌شوند، و محدودیتهایی را در انتخاب استراتژی برای عاملها ایجاد می‌کنند.

قوانین تسهیل کننده: قوانینی هستند که وضع می‌شوند تا رسیدن به اهداف اجتماعی را تسریع کنند و پاداش و پادافرهایی را برای عاملها در صورت انجام دادن استراتژیهای خاص در نظر می‌گیرند.

برای مثال، کتابخانه یک دانشگاه را در نظر بگیرید که در تابستان به دانشجویان کارشناسی کتاب امانت نمی‌دهد. با این که دانشجویان در تابستان کمتر به دانشگاه سر می‌زنند و ممکن است مدت زمانی که کتاب در اختیار آنها می‌ماند طولانی‌تر از زمان مجاز شود. فرض کنید که با دادن این تسهیلات در تابستان، از بین ۱۰۰ دانشجو ۹۹ نفر تخلف کنند و یک نفر در اثر استفاده از یک کتاب خوب بتواند در ۵ سال آینده سودی به اجتماع برساند که از ضرری که متخلفین وارد کرده اند بیشتر باشد، آنگاه وضع

این قانون بازدارنده کارایی سیستم را پایین آورده است. در این شرایط، قانون‌گذار با نگاه جلوگیری از

تخلف، قانون وضع کرده است نه با نگاه اینکه آیا این قانون کارایی سیستم را بالا می‌برد یا نه؟

اینکه قانونگذار چه نوع قانونی (بازدارنده یا تسهیل کننده) وضع کند مهم نیست. مهم آن است که قانونگذار بتواند اثبات کند که قوانین وضع شده کارایی سیستم را بالا می‌برد (البته باید ویژگی‌های دیگری چون سازگاری، تصمیم‌پذیری، عادلانه بودن، حسادت آزاد و ... نیز در نظر گرفته شود) برای این منظور باید منطق و روشی صوری تهیه دید که برهان افزایش کارایی را بتوان در آن ارائه داد. سیستم‌های هنجاری را به این منظور مورد مطالعه قرار می‌دهیم.

بطور کلی یک سیستم هنجاری عبارت از یک مجموعه از تکالیف و محدودیت‌های برای عملهای یک سیستم اجتماعی برای برآورده کردن اهدافی خاص است.

در این بخش منطق ^{۹۷} NTL ارائه شده در [۳] را برای سیستم‌های هنجاری معرفی می‌کنیم.

یک سیستم انتقالی $M = \langle S, \rightarrow, V \rangle$ را روی مجموعه At از فرمولهای اتمی در نظر بگیرید که

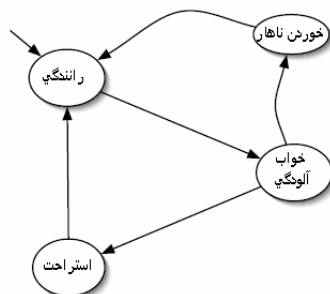
$\rightarrow$ یک رابطه سریال^{۹۸} باشد. در هر حالت از S ، یک عامل می‌تواند با توجه به رابطه انتقال $\rightarrow$

تصمیم بگیرد^{۹۹} که به چه حالت جدیدی منتقل شود.

^{۹۷} Normative Temporal Logic

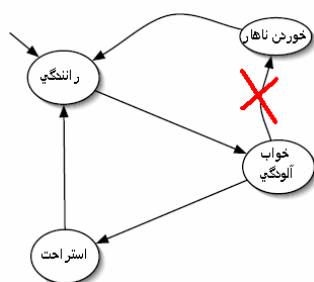
^{۹۸} یک رابطه $R \subset S \times S$ سریال است هرگاه $\forall s \exists t R(s, t)$.

^{۹۹} می‌توان همانند درخت بازی‌های به هر عضو S یک مجموعه از عالمها نسبت داد که مجاز به تصمیم‌گیری هستند ولی برای سادگی در اینجا این موضوع را در نظر نمی‌گیریم.



یک سیستم هنجاری روی سیستم انتقالی $M = \langle S, \rightarrow, V \rangle$ عبارت از (قانون) بازدارندگی

$\eta \subseteq \rightarrow$ است بطوریکه رابطه $\eta / \rightarrow$ یک رابطه سریال باشد. بازدارندگی η مشخص می‌کند که چه انتقالهایی از سیستم انتقالی مجاز نمی‌باشد. مجموعه بازدارندگی‌های رابطه $\rightarrow$ را با $N(\rightarrow)$ نمایش می‌دهیم.



برای بازدارندگی η ، یک مسیر (نامتناهی) π از سیستم انتقالی $M = \langle S, \rightarrow, V \rangle$ را مسیر η -آزاد

گوییم هرگاه هیچ‌یک از انتقالهای مسیر π در η نباشد. مجموعه مسیرهای η -آزاد سیستم انتقالی

M را که از حالت s آغاز می‌شود با $C_\eta(s)$ نمایش می‌دهیم. گوییم بازدارندگی η به اندازه

بازدارندگی μ گشوده است هرگاه $\mu \subseteq \eta$.

زبان منطق NTL

فرض کنید At یک مجموعه از فرمولهای اتمی و Γ مجموعه‌ای از نمادها (به منظور نمایش بازدارندگی‌ها در زبان منطق) باشد. مجموعه $L(At, \Gamma)$ ، فرمولهای زبان منطق NTL ، روی فرمولهای اتمی At و نمادهای بازدارندگی Γ ، کوچکترین مجموعه شامل At است بطوریکه

$$\varphi, \psi \in L(At, \Gamma) \Rightarrow \neg\varphi, \varphi \wedge \psi, P_\eta X\varphi, P_\eta(\varphi U \psi), O_\eta X\varphi, O_\eta(\varphi U \psi) \in L(At, \Gamma)$$

برای هر $\eta \in \Gamma$.

فرمولهای منطق بصورت زیر خوانده می‌شوند

$P_\eta X\varphi$: تحت بازدارندگی η ، جایز است که در گام بعدی φ .

$P_\eta(\varphi U \psi)$: تحت بازدارندگی η ، جایز است که ψ برقرار شود و تا زمانی که ψ برقرار شود φ برقرار

باشد.

$O_\eta X\varphi$: تحت بازدارندگی η ، واجب است که در گام بعدی φ .

$O_\eta(\varphi U \psi)$: تحت بازدارندگی η ، واجب است که ψ برقرار شود و تا زمانی که ψ برقرار شود φ

برقرار باشد.

معناشناسی منطق NTL

یک معناشناسی برای زبان $L(At, \Gamma)$ ، عبارت است از یک سیستم انتقالی $M = \langle S, \rightarrow, V \rangle$

$(V : S \rightarrow 2^{At})$ ، همراه با یک تعبیر $N(\rightarrow) : \Gamma \longrightarrow$ برای نمادهای بازدارندگی، که به هر

نماد بازدارندگی یک بازدارندگی روی رابطه $\rightarrow$ نسبت می‌دهد.

ارضا شدن گزاره‌های زبان $L(At, \Gamma)$ در مدل نقطه‌ای (M, s) با در نظر گرفتن تعبیر I بصورت زیر تعریف می‌شود.

$$(M, s) \models_I p \text{ iff } p \in V(s)$$

$$(M, s) \models_I \neg \varphi \text{ iff } (M, s) \not\models_I \neg \varphi$$

$$(M, s) \models_I \varphi \wedge \psi \text{ iff } (M, s) \models_I \varphi \ \& \ (M, s) \models_I \psi$$

$$(M, s) \models_I O_\eta X \varphi \text{ iff } \forall \pi \in C_{I(\eta)}(s) [(M, \pi^2) \models_I \varphi]$$

$$(M, s) \models_I P_\eta X \varphi \text{ iff } \exists \pi \in C_{I(\eta)}(s) [(M, \pi^2) \models_I \varphi]$$

$$(M, s) \models_I O_\eta(\varphi U \psi) \text{ iff } \forall \pi \in C_{I(\eta)}(s) [\exists k \in \mathbb{N} (M, \pi^k) \models_I \psi \ \& \ \forall t \leq k (M, \pi^t) \models_I \varphi]$$

$$(M, s) \models_I P_\eta(\varphi U \psi) \text{ iff } \exists \pi \in C_{I(\eta)}(s) [\exists k \in \mathbb{N} (M, \pi^k) \models_I \psi \ \& \ \forall t \leq k (M, \pi^t) \models_I \varphi]$$

تمرین. روی یک سیستم انتقالی (قانون) بازدارندگی را تعریف کردیم. یک **تسهیل‌کنندگی** روی

یک سیستم انتقالی $M = \langle S, \rightarrow, V \rangle$ عبارت است **تابع پادا** $\mathbb{R} \longrightarrow (\rightarrow) : \varsigma$ که به هر

انتقال یک عدد حقیقی به عنوان پاداش (در صورت مثبت بودن عدد) و به عنوان پادافره (در صورت

منفی بودن عدد) نسبت می‌دهد. اگر یک عامل یک انتقال را انجام دهد مقدار عدد داده شده را کسب

می‌کند. سعی کنید این مدل از سیستم‌های هنجاری را با نظریه بازی‌ها ترکیب کنید.

۵-۶ مدل سازی

مراجع

- [۱] فاطمه نبوی، منطق تکلیف با رویکرد اصول فقه، پایان نامه دکتری دانشگاه صنعتی شریف، ۱۳۸۸
- [2] J. F. Horty. **Agency and Deontic Logic**, Oxford University Press, 2001
- [3] T. Agotnes, W. van der Hoek, and ..., *On the Logic of Normative Systems*, 2007.
- [4].

۷

منطق زمانی

مقدمه

عامل‌ها یک سیستم اجتماعی در زمان زیست می‌کنند. به این ترتیب که سیستم اجتماعی از یک وضعیت اجتماعی به یک وضعیت دیگر اجتماعی منتقل می‌شود. برای نمونه، در منطق شناختی، عمل‌ها شناختی وضعیت آگاهی عامل‌ها را تغییر می‌دادند و در نظریه بازی‌ها تکاملی عامل‌ها می‌توانند تکامل پیدا کنند، یا جدول سود بازی از وضعیتی به وضعیتی دیگر تغییر کند. برای اینکه بتوانیم در مورد آینده سیستم استدلال کنیم نیاز به موجهات زمانی داریم که منطق زمانی آن‌ها را فراهم می‌سازد. منطق زمانی با منطق‌های دیگر چون منطق تکلیف (به هدف استدلال در مورد تعهد آینده عالم‌ها در طول زمان)، منطق شناختی (به هدف استدلال در مورد آگاهی آینده عالم‌ها در طول زمان) و روش‌های صوری دیگر به منظور زمانی کردن آنها ترکیب شده است.

(این فصل کامل نیست و با اهداف درس برای سیستم‌های اجتماعی فاصله زیادی دارد. باید کاربردهای اجتماعی و نظریه‌های ترکیبی به آن اضافه شود)

۷-۱ سیستم‌های انتقالی

سیستم انتقالی^{۱۰۰} یک سیستم چند وضعیتی است که از وضعیتی به وضعیتهای دیگر منتقل می‌شود. می‌توان موارد زیادی را به عنوان سیستم‌های انتقالی در نظر گرفت، همانند: اجرای یک برنامه کامپیوتری که با انجام هر دستور از وضعیتی (مقادیر متغیرها) به وضعیت دیگر (مقادیر جدید) منتقل می‌شود، یک پروتکل ارتباطی که با انجام هر ارتباط وضعیت آگاهی عامل‌ها تغییر می‌کند، یک وسیله

مکانیکی که اهرم‌ها و چرخ‌دنده‌هایش از وضعیتی به وضعیتی دیگر منتقل می‌شوند، یک حرکت اجتماعی و

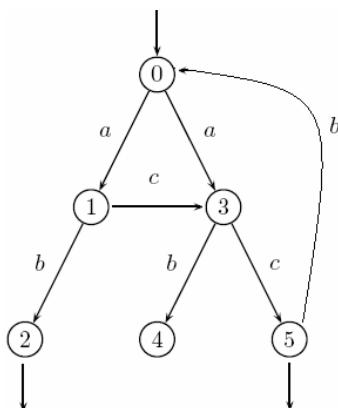
سیستم‌های انتقالی برای منطق زمانی همان نقشی را بازی می‌کنند که مدل‌های کریپکی دانش برای منطق شناختی بازی می‌کنند (از این رو، به سیستم‌های انتقالی مدل‌های کریپکی نیز گفته می‌شود). در این بخش به تعریف سیستم‌های انتقالی برچسب‌دار و اینکه چگونه یک سیستم انتقالی بزرگ را می‌توان به صورت ترکیب چند سیستم انتقالی کوچکتر که با هم تعامل می‌کنند نوشت، خواهیم پرداخت.

تعریف ۷-۱-۱. یک سیستم انتقالی برچسب‌دار T عبارت است از چندتایی $(S, A, \rightarrow, \downarrow, s_0)$ که

- S یک مجموعه از وضعیتهای سیستم است،
- A یک مجموعه از عمل‌ها است.
- $\rightarrow \subseteq S \times A \times S$ رابطه انتقال سیستم است. برای $(s, a, t) \in \rightarrow$ می‌نویسم $s \xrightarrow{a} t$ و این یعنی از وضعیت s می‌توان با انجام عمل a به وضعیت t منتقل شد.
- $\downarrow \subseteq S$ مجموعه وضعیت‌های موفق سیستم است.
- $s_0 \in S$ وضعیت آغازین سیستم است.

نکته. الف. می‌توان به تعریف سیستم انتقالی، در صورت نیاز برای مدل‌سازی سیستم‌های اجتماعی، یک مجموعه از عامل‌ها نیز اضافه کرد. ب. فرض می‌کنیم که سیستم‌های انتقالی همبند هستند، یعنی هر وضعیتی قابل دسترسی از وضعیت آغازین است.

مثال ۷-۱-۲. سیستم انتقالی شکل را ببینید.



مجموعه وضعیتها $S = \{0, 1, 2, 3, 4, 5\}$ ، مجموعه $A = \{a, b, c\}$ ، $s_0 = 0$ ، $\downarrow = \{2, 5\}$ و رابطه انتقال مطابق شکل مشخص می‌شود.

نمادگذاری. برای مجموعه عمل‌های A ، A^* را مجموعه همه رشته‌ها بطول متناهی روی الفبای A می‌گیریم. $\lambda \in A^*$ رشته به طول صفر است. برای $s, t \in S$ و $\sigma \in A^*$ ، $s \xrightarrow{\sigma}^* t$ یعنی اینکه می‌توان با انجام دادن عمل‌ها در رشته σ از وضعیت s به t منتقل شد.

هم‌ارزی سیستم‌های انتقالی

چه موقع دو سیستم انتقالی با هم برابر (هم‌ارز) فرض می‌شوند؟ می‌توان حداقل ۴ نوع هم‌ارزی برای سیستم‌های انتقالی نام برد ۱- یکریختی گرافی ۲- هم‌ارزی زبانی 1,1 ۳- هم‌ارزی مسیری 1,2 و ۴- هم-شبه‌سازی 1,3 .

تعریف ۷-۱-۳. برای سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ ، قرار می‌دهیم

مسیرهای موفقیت: $L(T) = \{\sigma \in A^* \mid \exists t \in S (t \in \downarrow \wedge s_0 \xrightarrow{\sigma} t)\}$

مسیرهای ممکن: $Trace(T) = \{\sigma \in A^* \mid \exists t \in S (s_0 \xrightarrow{\sigma} t)\}$

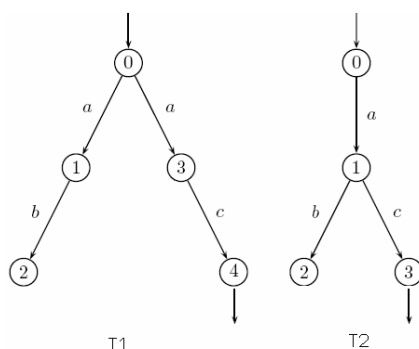
دو سیستم انتقالی $T' = (S', A', \rightarrow', \downarrow', s_0')$, $T = (S, A, \rightarrow, \downarrow, s_0)$

۱. هم‌ارز زبانی هستند هرگاه $L(T) = L(T')$

۲. هم‌ارز مسیری هستند هرگاه $Trace(T) = Trace(T')$ و $L(T) = L(T')$

تمرین. بررسی کنید که یکرختی گرافی هم‌ارزی مسیری، و هم‌ارزی مسیری هم‌ارزی زبانی را نتیجه می‌دهد و نه برعکس.

مثال ۷-۱-۴. دو سیستم انتقالی در شکل زیر را در نظر بگیرید.



دو سیستم انتقالی T_1, T_2 هم‌ارز مسیری (و در نتیجه هم‌ارز زبانی) هستند. اما با این وجود این دو سیستم با هم متفاوتند. فرض کنید که هر گره غیر پایانی در سیستم‌های انتقالی یک گره تصمیم‌گیری باشد بطوریکه گره 0 در هر دو سیستم انتقالی گره تصمیم‌گیری عامل یک، گره 1 در هر دو سیستم انتقالی گره تصمیم‌گیری عامل دو، و همچنین گره 3 نیز گره تصمیم‌گیری عامل دو باشد. با اینکه دو سیستم انتقالی هم‌ارز مسیری هستند، اما در سیستم انتقالی T_1 ، تصمیم‌گیری عامل یک مسیر نهایی را مشخص می‌کند، در حالیکه در سیستم انتقالی T_2 ، تصمیم‌گیری عامل دو مسیر نهایی را مشخص می‌کند.

تعریف ۷-۱-۵. گوییم سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ سیستم انتقالی

$T' = (S', A', \rightarrow', \downarrow', s'_0)$ را شبیه‌سازی می‌کند هرگاه رابطه (شبیه‌ساز کننده) $R \subseteq S \times S'$

وجود داشته باشد که خواص زیر را دارا است

۱. $(s_0, s'_0) \in R$. (وضعیت‌های آغازین دو سیستم با هم در رابطه باشند)،

۲. اگر $(s, s') \in R$ و $s' \xrightarrow{a} t'$ آنگاه وضعیت $t \in S$ باشد بطوریکه $s \xrightarrow{a} t$ و

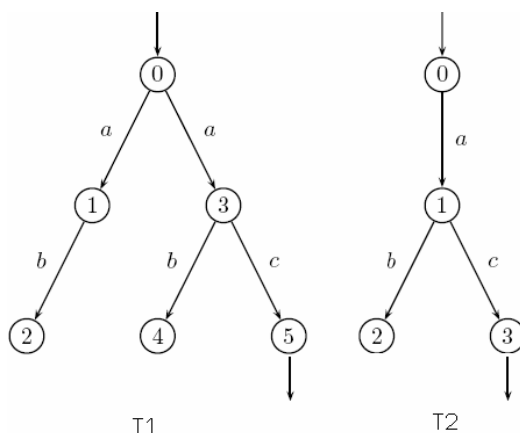
$(t, t') \in R$. (یعنی، اگر دو وضعیت $s \in S$ و $s' \in S'$ با هم در رابطه باشند و بتوان در

وضعیت s' عمل a را در سیستم T' انجام داد و به وضعیت t رسید آنگاه از وضعیت s

بتوان اینکار را شبیه‌سازی کرد)

۳. هرگاه $s' \in \downarrow'$ و $(s, s') \in R$ آنگاه $s \in \downarrow$

مثال ۷-۱-۶. دو سیستم انتقالی در شکل زیر را در نظر بگیرید.



نشان دهید

الف. سیستم انتقالی $T1$ سیستم انتقالی $T2$ را شبیه‌سازی می‌کند. (فرض کنید که شما در وضعیت آغاز

سیستم انتقالی $T1$ و دوست شما در وضعیت آغاز سیستم انتقالی $T2$ قرار دارد. دوست شما در $T2$ هر عملی را

انجام دهد و به وضعیت دیگری منتقل شود شما می‌توانید همان عمل را انجام دهید و به وضعیتی در $T1$ منتقل شوید که باز هم بتوانید عملهای ممکن آینده دوستان را تقلید کنید)

ب. سیستم انتقالی $T2$ سیستم انتقالی $T1$ را شبیه‌سازی می‌کند.

ج. دو سیستم انتقالی $T1$ و $T2$ هم‌ارز مسیری هستند.

تمرین. نشان دهید اگر دو سیستم انتقالی همدیگر را شبیه‌سازی کنند آنگاه با هم هم‌ارز مسیری هستند.

تعریف ۷-۱-۷. گوییم دو سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ و

$$T' = (S', A', \rightarrow', \downarrow', s'_0)$$

$R \subseteq S \times S'$ (هم‌شبیه‌ساز کننده) رابطه (هم‌شبیه‌ساز هستند هرگاه

وجود داشته باشد که خواص زیر را دارا است

$$1. (s_0, s'_0) \in R. \text{ (وضعیت‌های آغازین دو سیستم با هم در رابطه باشند),}$$

$$2. \text{ اگر } (s, s') \in R \text{ و } s' \xrightarrow{a} t' \text{ آنگاه وضعیت } t \in S \text{ باشد بطوریکه } s \xrightarrow{a} t, \text{ و}$$

$$(t, t') \in R$$

$$3. \text{ اگر } (s, s') \in R \text{ و } s \xrightarrow{a} t \text{ آنگاه وضعیت } t' \in S' \text{ باشد بطوریکه } s' \xrightarrow{a} t', \text{ و}$$

$$(t, t') \in R$$

$$4. \text{ هرگاه } s' \in \downarrow' \text{ و } (s, s') \in R \text{ آنگاه } s \in \downarrow$$

$$5. \text{ هرگاه } s \in \downarrow \text{ و } (s, s') \in R \text{ آنگاه } s' \in \downarrow'$$

تمرین. رابطه هم‌شبیه‌سازی را می‌توان برای هر نوع از مدل‌های کریپکی تعریف کرد. تعریف رابطه هم-شبیه‌سازی را برای مدل‌های کریپکی منطق‌شناختی جستجو کنید. نشان دهید اگر دو مدل نقطه‌ای کریپکی دانش با هم هم‌شبیه‌ساز باشند آنگاه فرمول‌های یکسانی را ارضا می‌کنند. با مثال نقض نشان دهید عکس این موضوع برقرار نیست.

تمرین. نشان دهید که اگر دو سیستم انتقالی هم‌شبیه‌ساز باشند آنگاه همدیگر را شبیه‌سازی می‌کنند. عکس این موضوع برقرار نیست. به سیستم‌های انتقالی مثال ۷-۱-۵ توجه کنید.

برهم‌کنش^{۱۰۴}

فرض کنید بخواهیم یک سیستم واقعی (یک برنامه کامپیوتری، یک سخت‌افزار، یک پروتکل ارتباطی، یک سیستم اقتصادی) را بصورت یک سیستم انتقالی مدل کنیم. سیستم واقعی می‌تواند بسیار پیچیده و تعداد وضعیت‌های ممکن و انتقال‌های آن بطور قابل توجهی عددی بزرگ باشد، به نحوی که ارائه یک سیستم انتقالی به عنوان مدل سیستم واقعی دشوار باشد. برای حل این دشواری، اگر سیستم واقعی را به این صورت نگاه کنیم که سیستم واقعی از برهم‌کنش چند سیستم کوچکتر بدست می‌آید، آنگاه هر سیستم کوچکتر را با یک سیستم انتقالی مدل می‌کنیم و با استفاده از عملگرهای ترکیب سیستم‌های انتقالی، مدل سیستم انتقالی برای سیستم واقعی مورد نظر را می‌سازیم.

برهم‌کنش چیست؟ هر عمل ساده را می‌توان به دو بخش تقسیم کرد: کنش و واکنش. فرض کنید که لیوانی را برمی‌دارید. این برداشتن را می‌توان به صورت زیر دید که این عمل از برهم‌کنش دو بخش بدست می‌آید.

۱. بخش کنش که شما آن را انجام می‌دهید،

۲. بخش واکنش که لیوان آن را انجام می‌دهد.

مثالی دیگر، فرض کنید با گچ خطی بر تخته سیاه کشیده می‌شود. کشیده شدن خط از برهم‌کنش دو

بخش بدست می‌آید

۱. بخش کنش که گچ آن را انجام می‌دهد،

۲. بخش واکنش که تخته آن را انجام می‌دهد.

با این نگاه، هر عمل یک برهم‌کنش از دو عمل کنش و واکنش است. آنچه پدیدار می‌شود برهم‌کنش

است. کنش و واکنش پدیده سازند^{۱۰۵}.

به این ترتیب وقتی با یک سیستم واقعی پیچیده روبرو هستیم، می‌توانیم عمل‌های آن را بصورت برهم-

کنش عملهای چند سیستم ساده‌تر در نظر بگیریم. سیستم‌های ساده را به کمک سیستم‌های انتقالی

مدل کنیم و با عملگرهای ترکیب مدل سیستم واقعی را بدست آوریم.

تعریف ۷-۱-۸. یک تابع برهم‌کنش^{۱۰۶} روی مجموعه عملهای A عبارت است از تابع

جزیی $\gamma : A \times A \rightarrow A$ بطوریکه $\gamma(a, b) = \gamma(b, a)$ برای هر $a, b \in A$. (در اینجا، برای

سادگی فرض می‌کنیم که برای عمل‌های در برد γ ، تابع γ تعریف نشده است، یعنی $\gamma(c, \gamma(b, a))$

تعریف نشده است.)

¹⁰⁵ آنچه آن را پدیده (واقعیت) می‌نامم، چیزی جز برهم‌کنش اندیشدین من با آفرینه نیست. برای آنکه پدیده دیگری را تجربه کنم، کافیت اندیشدینی تازه را آغاز کنم.

¹⁰⁶ در نظریه پردازها (process theory) مراجع [؟،؟] communication function نامیده می‌شود.

برای دو عمل $a, b \in A$ ، $\gamma(a, b)$ (در صورتی که تعریف شده باشد) برهم‌کنش دو عمل a, b است. از آنجا که فرض می‌کنیم $\gamma(a, b) = \gamma(b, a)$ ، تفاوتی ندارد a را کنش و b را واکنش، یا b را کنش و a را واکنش بدانیم.

تعریف ۷-۱-۹. دو سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ و $T' = (S', A', \rightarrow', \downarrow', s_0')$ را همراه با یک تابع برهم‌کنش γ روی مجموعه عمل‌های $A \cup A'$ در نظر بگیرید. **ترکیب موازی**^{۱۰۷}

T و T' تحت برهم‌کنشی γ ، سیستم انتقالی $T'' = (S'', A'', \rightarrow'', \downarrow'', s_0'')$ که

$$S'' = S \times S' \quad ۱.$$

$$A'' = A \cup A' \cup \{ \gamma(a, b) \mid a \in A, b \in A' \} \quad ۲.$$

است و می‌تواند برای هیچ زوج مرتبی تعریف نشده باشد و مجموعه سوم در اجتماع بالا تهی باشد

۳. رابطه انتقال سیستم T'' ، $\rightarrow'' \subseteq S'' \times A'' \times S''$ ، کوچکترین مجموعه‌ای است که برای

$$\text{هر } s, t \in S, s', t' \in S, a \in A, b \in A' \text{ هر}$$

$$\text{الف. اگر } s \xrightarrow{a} t \text{ آنگاه } (s, s') \xrightarrow{a}'' (t, s')$$

$$\text{ب. اگر } s' \xrightarrow{b} t' \text{ آنگاه } (s, s') \xrightarrow{b}'' (s, t')$$

$$\text{ج. اگر } s \xrightarrow{a} t \text{، } s' \xrightarrow{b} t' \text{ و } \gamma(a, b) \text{ تعریف شده باشد آنگاه}$$

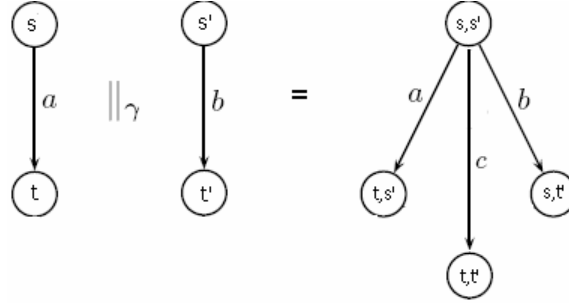
$$(s, s') \xrightarrow{\gamma(a, b)}'' (t, t')$$

$$\downarrow'' = \downarrow \times \downarrow' \quad ۴.$$

$$s_0'' = (s_0, s_0') \quad ۵.$$

T'' ترکیب موازی T و T' تحت برهم کنشی γ را با نماد $T \parallel_\gamma T'$ نمایش می دهیم.

مثال ۷-۱-۱۰. در شکل زیر، تابع برهم کنشی $\gamma(a, b) = c$ است.



فرض کنید که در شکل مثال ۷-۱-۹، عمل a کنشی باشد که گچ آن را انجام می دهد و عمل b واکنشی باشد که تخته آن را انجام می دهد. عمل c (برهم کنش a, b) آن است که پدیده می شود.

تعریف ۷-۱-۱۱. سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ را همراه با مجموعه $H \subseteq A$ در نظر

بگیرید. **پدیده سازی** T^{p} با توجه به مجموعه H ، سیستم انتقالی $T' = (S', A', \rightarrow', \downarrow', s_0')$

است که

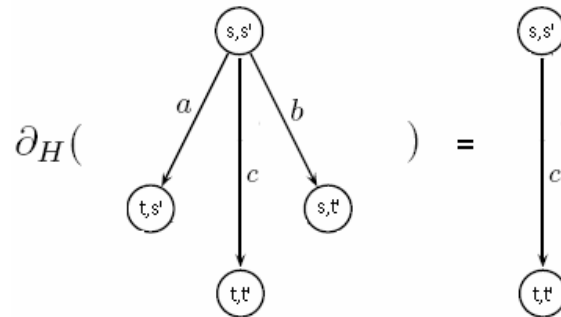
$$۱. \quad A' = A, S' = S$$

$$۲. \quad s_0' = s_0, \downarrow' = \downarrow|_{S'}$$

$$۳. \quad \rightarrow' = \rightarrow \cap (S \times (A - H) \times S)$$

سیستم انتقالی T' را با نماد $\delta_H(T)$ نمایش می دهیم.

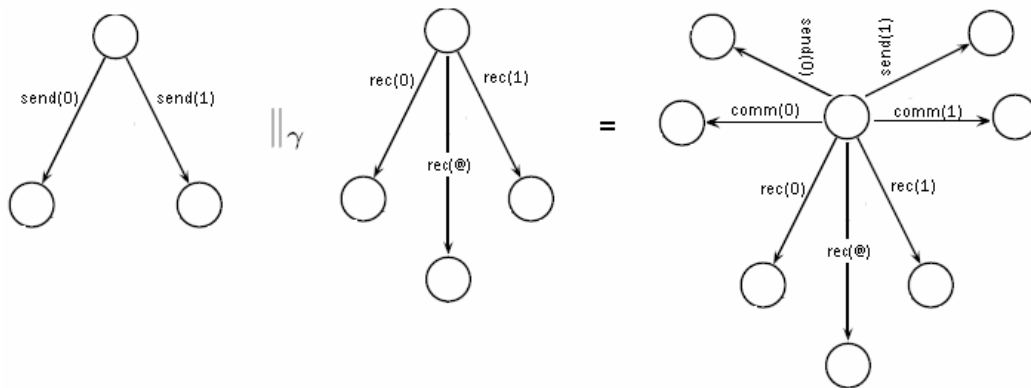
مثال ۷-۱-۱۲. در شکل زیر، $H = \{a, b\}$ است.



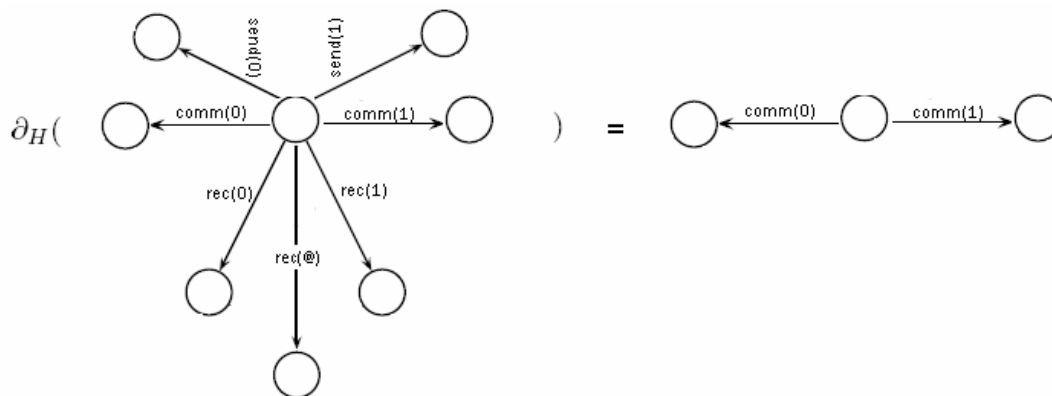
فرض کنید که دوست خود را در خیابان می بینید و به او سلام می کنید. در شکل مثال ۷-۱-۹، عمل a را گفتن سلام توسط شما، و عمل b را شنیدن سلام توسط دوستان تصور کنید. برهم کنش a, b را با c نمایش دهید. اگر بخواهید از عملهای کنش و واکنش a, b صرف نظر کنید و فقط c را در نظر بگیرید. می توانید عمل پدیده سازی شکل مثال ۷-۱-۱۱ را انجام دهید.

مثال ۷-۱-۱۳. دو عامل را در نظر بگیرید که یکی فرستنده است و دیگری گیرنده. عامل فرستنده یا

نماد 0 یا 1 را می فرستد. عامل گیرنده یا نماد 0 یا 1 یا @ را دریافت می کند.



تابع برهم‌کنشی $\gamma(send(i), rec(i)) = comm(i)$ برای $i \in \{0,1\}$ تعریف می‌شود. برای مجموعه عملهای $H = \{rec(0), rec(1), rec(@), send(0), send(1)\}$ پدیده‌سازی بصورت شکل زیر خواهد بود.



در تعریف ۷-۱-۹، عملگر ترکیب موازی را برای سیستم‌موازی معرفی کردیم. در ادامه، دو عملگر ترکیب انتخابی^{۱۰۹} و ترکیب پیاپی^{۱۱۰} را معرفی می‌کنیم.

تعریف ۷-۱-۱۴. دو سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ و $T' = (S', A', \rightarrow', \downarrow', s'_0)$ را

که $S \cap S' = \emptyset$ در نظر بگیرید. **ترکیب انتخابی** T, T' ، سیستم انتقالی

$$T'' = (S'', A'', \rightarrow'', \downarrow'', s_0'')$$

$$1. \quad S'' = \{s_0''\} \cup S \cup S' \quad \text{که } s_0'' \notin S \cup S'$$

$$2. \quad A'' = A \cup A'$$

۳. رابطه انتقال سیستم T'' ، $\rightarrow'' \subseteq S'' \times A'' \times S''$ ، کوچکترین مجموعه‌ای است که برای

$$\text{هر } t \in S, t' \in S', a \in A, b \in A'$$

$$\text{الف. اگر } s_0 \xrightarrow{a} t \text{ آنگاه } s_0'' \xrightarrow{a} t''$$

$$\text{ب. اگر } s_0' \xrightarrow{b} t' \text{ آنگاه } s_0'' \xrightarrow{b} t''$$

$$\text{ج. } \rightarrow' \subseteq \rightarrow''$$

۴. $\downarrow''$ کوچکترین مجموعه‌ای که $\downarrow' \subseteq \downarrow''$ و اگر $s_0 \in \downarrow$ یا $s_0' \in \downarrow'$ آنگاه $s_0'' \in \downarrow''$

ترکیب انتخابی T, T' را با نماد $T + T'$ نمایش می‌دهیم.

ترکیب انتخابی $T + T'$ یعنی می‌توان انتخاب کرد که سیستم انتقالی T را دنبال کرد یا سیستم-

انتقالی T' را.

تعریف ۷-۱-۱۵. دو سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ و $T' = (S', A', \rightarrow', \downarrow', s_0')$ را

که $S \cap S' = \emptyset$ در نظر بگیرید. ترکیب پیایی T', T ، سیستم انتقالی

$$T'' = (S'', A'', \rightarrow'', \downarrow'', s_0'')$$

$$1. S'' = S \cup S'$$

$$2. A'' = A \cup A'$$

۳. رابطه انتقال سیستم T'' ، $\rightarrow'' \subseteq S'' \times A'' \times S''$ ، کوچکترین مجموعه‌ای است که برای

$$\text{هر } s \in \downarrow, t' \in S', b \in A'$$

$$\text{الف. اگر } s_0' \xrightarrow{b} t' \text{ آنگاه } s \xrightarrow{b} t''$$

$$\text{ب. } \rightarrow' \subseteq \rightarrow''$$

۴. $\downarrow''$ کوچکترین مجموعه‌ای که $\downarrow' \subseteq \downarrow''$ و اگر $s'_0 \in \downarrow'$ آنگاه $\downarrow \subseteq \downarrow''$

$$s''_0 = s_0 \quad ۵.$$

ترکیب پیایی T', T را با نماد $T.T'$ نمایش می‌دهیم.

ترکیب پیایی $T.T'$ یعنی اول سیستم انتقالی T را دنبال می‌کنیم و از وضعیت‌های موفقیت T آغاز به دنبال کردن سیستم انتقالی T' می‌کنیم.

تمرین. عملگری تعریف کنید که سیستم انتقالی را به تکرار و می‌دارد. یعنی سیستم انتقالی پس از رسیدن به وضعیت‌های موفق دوباره خودش را فراخوانی می‌کند.

تمرین. نماد $\equiv$ را برای رابطه هم‌شبه‌سازی بین سیستم‌های انتقالی در نظر بگیرید. نشان دهید که

رابطه هم‌شبه‌سازی با عملگرهای ترکیبی همخوان است. یعنی اگر $T_1 \equiv T'_1$, $T_2 \equiv T'_2$ آنگاه

$$T_1 + T_2 \equiv T'_1 + T'_2 \quad \text{I}$$

$$T_1.T_2 \equiv T'_1.T'_2 \quad \text{II}$$

$$T_1 \parallel_\gamma T_2 \equiv T'_1 \parallel_\gamma T'_2 \quad \text{III}$$

$$\delta_H(T_1) \equiv \delta_H(T'_1) \quad \text{IV}$$

عمل ساکت^{۱۱۱}

می‌خواهیم بعضی از عمل‌های یک سیستم انتقالی را درونی کنیم یا از دید یک عامل نهان‌سازی کنیم. برای این منظور عمل ساکت τ را به عنوان یک عمل جدید در نظر می‌گیریم. تابع نهان‌سازی بصورت زیر تعریف می‌شود.

تعریف ۷-۱-۱۶. سیستم انتقالی $T = (S, A, \rightarrow, \downarrow, s_0)$ و مجموعه $I \subset A$ را در نظر بگیرید

نهان‌سازی^{۱۱۲} عملهای I در T ، سیستم انتقالی $T' = (S', A', \rightarrow', \downarrow', s'_0)$

است که

$$1. A' = A \cup \{\tau\}, S' = S$$

$$2. s'_0 = s_0, \downarrow' = \downarrow$$

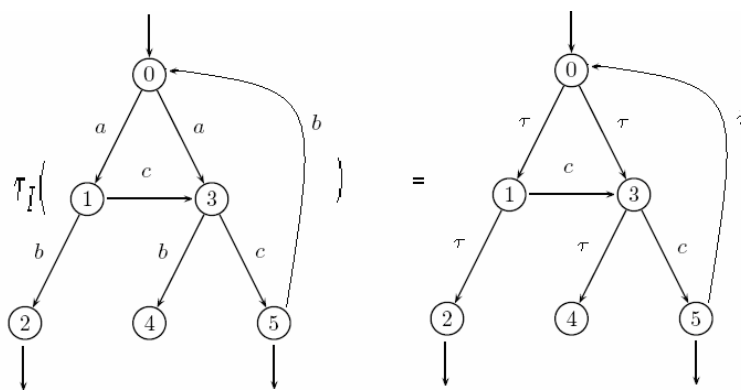
$$3. \rightarrow' \subseteq S' \times A' \times S'$$

الف. اگر $s \xrightarrow{a} t$ و $a \in I$ آنگاه $s \xrightarrow{\tau} t$

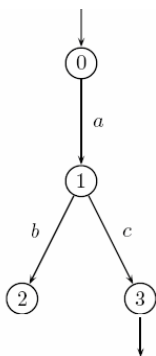
ب. اگر $s \xrightarrow{a} t$ و $a \notin I$ آنگاه $s \xrightarrow{a} t$

سیستم انتقالی T' را با نماد $\tau_I(T)$ نمایش می‌دهیم.

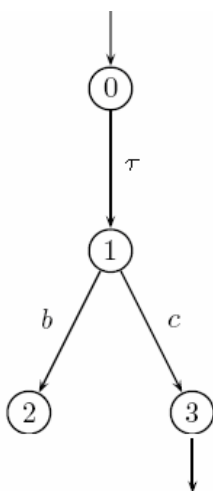
مثال ۷-۱-۱۷. در شکل زیر مجموعه $I = \{a, b\}$ است.



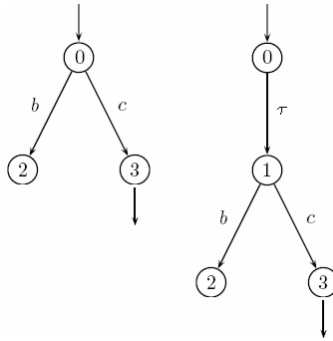
سیستم انتقالی زیر را در نظر بگیرید.



فرض کنید که عمل a را از دید ناظر بیرونی نهان سازی (درونی سازی) کنیم.



ناظر بیرونی تفاوتی بین دو سیستم انتقالی زیر نمی تواند بگذارد.



برای مثال، فرض کنید که دوست شما همیشه اول با همسرش مشورت می‌کند (a) و بعد یا به شما (b) می‌رود و یا به اسب سواری (c). اگر عمل a درونی باشد و از دید شما نهان باشد، آنگاه شما نمی‌توانید بین دو سیستم انتقالی در شکل بالا تمییز دهید، که آیا b, c بعد از عملی که از دید شما نهان است قابل اجرا هستند یا نه؟ در زیر تعریفی از هم‌شبه‌سازی برای این منظور ارائه می‌دهیم. در ادامه، منظور از مجموعه A_τ این است که $\tau \in A_\tau$ ؛ یعنی عمل ساکت نیز به عنوان یک برچسب عمل در سیستم انتقالی در نظر گرفته می‌شود.

تعریف ۷-۱-۱۸. گوییم دو سیستم انتقالی $T = (S, A_\tau, \rightarrow, \downarrow, s_0)$ و

$T' = (S', A'_\tau, \rightarrow', \downarrow', s'_0)$ هم‌شبه‌ساز شاخه‌ای^{۱۱۳} هستند هرگاه رابطه (هم‌شبه‌ساز کننده

شاخه‌ای) $R \subseteq S \times S'$ وجود داشته باشد که خواص زیر را دارا است

۱. $(s_0, s'_0) \in R$. (وضعیت‌های آغازین دو سیستم با هم در رابطه باشند)،

۲. اگر $(s, s') \in R$ و برای یک $a \in A'_\tau$ ، $s' \xrightarrow{a} t'$ ، آنگاه

یا $a = \tau$ و $(s, t') \in R$

یا وجود دارد $v, t \in S$ و یک دنباله بطول صفر یا بیشتر از انتقال‌های ساکت، که

$$s \xrightarrow{\tau} \dots \xrightarrow{\tau} v$$

بطوریکه $(v, s') \in R$ ، $v \xrightarrow{a} t$ و $(t, t') \in R$.

۳. اگر $(s, s') \in R$ و برای یک $a \in A_\tau$ ، $s \xrightarrow{a} t$ ، آنگاه

یا $a = \tau$ و $(t, s') \in R$

یا وجود دارد $v', t' \in S'$ و یک دنباله بطول صفر یا بیشتر از انتقال‌های ساکت، که

$$s' \xrightarrow{\tau} \dots \xrightarrow{\tau} v'$$

بطوریکه $(s, v') \in R$ ، $v' \xrightarrow{a} t'$ و $(t, t') \in R$.

۴. هرگاه $s' \in \downarrow'$ و $(s, s') \in R$ آنگاه وجود دارد $v \in S$ و یک دنباله بطول صفر یا بیشتر از

انتقال‌های ساکت، که

$$s \xrightarrow{\tau} \dots \xrightarrow{\tau} v$$

بطوریکه $(v, s') \in R$ و $v \in \downarrow$

۵. هرگاه $s \in \downarrow$ و $(s, s') \in R$ آنگاه وجود دارد $v' \in S'$ و یک دنباله بطول صفر یا بیشتر

از انتقال‌های ساکت، که

$$s' \xrightarrow{\tau} \dots \xrightarrow{\tau} v'$$

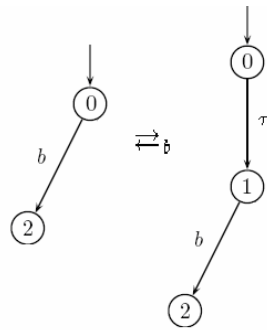
بطوریکه $(s, v') \in R$ و $v' \in \downarrow'$

نماد $T \rightleftharpoons_b T'$ را برای بیان اینکه دو سیستم انتقالی T, T' با هم هم‌شبه‌ساز شاخه‌ای هستند

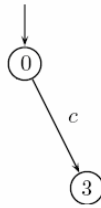
استفاده می‌کنیم.

تمرین. متاسفانه هم‌شبه‌سازی شاخه‌ای با عملگرهای ترکیب سیستم‌های انتقالی همخوانی ندارد. دو

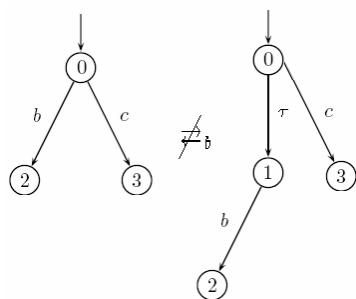
سیستم انتقالی زیر را در نظر بگیرید.



این دو سیستم با هم هم‌شبه‌ساز شاخه‌ای هستند. ولی اگر هر دو آنها را با سیستم زیر ترکیب‌انتخابی کنیم،



سیستم‌های حاصل با هم هم‌شبه‌ساز شاخه‌ای نیستند.



چرا؟

تعریف ۷-۱-۱۹. گوییم دو سیستم انتقالی $T = (S, A_T, \rightarrow, \downarrow, s_0)$ و

$$T' = (S', A'_T, \rightarrow', \downarrow', s'_0)$$
 هم‌شبه‌ساز شاخه‌ای ریشه‌ای^{۱۱۴} هستند هرگاه رابطه

$R \subseteq S \times S'$ وجود داشته باشد که اولاً هم‌شبه‌ساز کننده شاخه‌ای باشد و در شرایط (شرایط ریشه) زیر صدق کند.

(a) برای هر $a \in A_T$ و $t \in S$ اگر $s_0 \xrightarrow{a} t$ آنگاه $t' \in S'$ باشد که

$$(t, t') \in R \text{ و } s'_0 \xrightarrow{a'} t'$$

(b) برای هر $a \in A'_T$ و $t' \in S'$ اگر $s'_0 \xrightarrow{a'} t'$ آنگاه $t \in S$ باشد که

$$(t, t') \in R \text{ و } s_0 \xrightarrow{a} t$$

(c) $s'_0 \in \downarrow'$ اگر و تنها اگر $s_0 \in \downarrow$

نماد $T \rightleftharpoons_{rb} T'$ را برای بیان اینکه دو سیستم انتقالی T, T' با هم هم‌شبه‌ساز شاخه‌ای ریشه‌ای

هستند استفاده می‌کنیم.

تمرین. نشان دهید که رابطه هم‌شبه‌سازی شاخه‌ای ریشه‌ای با عملگرهای ترکیبی همخوان است.

یعنی اگر $T_1 \rightleftharpoons_{rb} T'_1, T_2 \rightleftharpoons_{rb} T'_2$ آنگاه

$$T_1 + T_2 \rightleftharpoons_{rb} T'_1 + T'_2 \quad \text{I}$$

$$T_1.T_2 \rightleftharpoons_{rb} T'_1.T'_2 \quad \text{II}$$

$$T_1 \parallel_\gamma T_2 \rightleftharpoons_{rb} T'_1 \parallel_\gamma T'_2 \quad \text{III}$$

$$\delta_H(T_1) \rightleftharpoons_{rb} \delta_H(T'_1) \quad \text{IV}$$

$$V. \tau_I(T_1) \xrightarrow{rb} \tau_I(T'_1)$$

منطق Hennessy-Milner

منطق زیر این امکان را فراهم می‌سازد تا بتوانیم خواصی از سیستم‌های انتقالی را توصیف کنیم. می‌توان ثابت کرد که دو سیستم انتقالی برچسب‌دار هم‌شبه‌ساز هستند اگر و تنها اگر فرمول‌های یکسانی از منطق Hennessy-Milner [۴] را ارضا کنند.

.....

...

مدلسازی شام خوردن فیلسوفان

مساله همزمانی ۲-۵-۱، شام خوردن فیلسوفان را در نظر بگیرید.



مجموعه عملهای A به صورت زیر تعریف می‌شود.

$$\begin{aligned}
A = & \left\{ pick_i(j) \mid j \in \{i, i \oplus 1\}, 0 \leq i \leq 4 \right\} \cup \\
& \left\{ put_i(j) \mid j \in \{i, i \oplus 1\}, 0 \leq i \leq 4 \right\} \cup \\
& \left\{ picked_i \mid 0 \leq i \leq 4 \right\} \cup \\
& \left\{ Lhand_i, Rhand_i, eat_i \mid 0 \leq i \leq 4 \right\} \cup \\
& \left\{ table_i \mid 0 \leq i \leq 4 \right\}
\end{aligned}$$

که $\oplus$ جمع در مبنای 5 است.

معنای غیر صوری هر عمل بصورت زیر است.

$pick_i(j)$: فیلسوف i چنگال j را از روی میز برمی دارد.

$put_i(j)$: فیلسوف i چنگال j را روی میز می گذارد.

$picked_i$: چنگال i برداشته می شود.

put_i : چنگال i گذاشته می شود.

$Lhand_i$: فیلسوف i چنگال در دست چپش می گیرد

$Rhand_i$: فیلسوف i چنگال در دست راستش می گیرد.

eat_i : فیلسوف i در حال خوردن شام است.

$table_i$: چنگال i روی میز قرار می گیرد.

تابع برهم کنشی $\gamma : A \times A \rightarrow A$ را به صورت زیر در نظر می گیریم.

$$\gamma(pick_i(i), picked_i) = Lhand_i$$

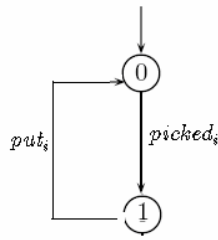
$$\gamma(pick_i(i \oplus 1), picked_{i \oplus 1}) = Rhand_i$$

$$\gamma(Lhand_i, Rhand_i) = eat_i$$

$$\gamma(put_i(j), put_j) = table_j$$

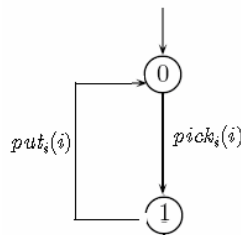
سه نوع سیستم انتقالی در نظر می گیریم: سیستم انتقالی چنگال، سیستم انتقالی دست چپ، سیستم-
انتقالی دست راست.

سیستم انتقالی چنگال i $(FORK^i)$:



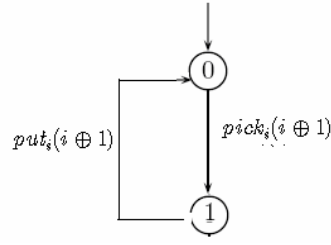
(یک چنگال برداشته و گذاشته می شود)

سیستم انتقالی دست چپ فیلسوف i $(LEFT^i)$:



(دست چپ چنگال سمت خود را برمی دارد و می گذارد)

سیستم انتقالی دست راست فیلسوف i ($RIGHT^i$):



(دست راست چنگال سمت خود را برمی دارد و می گذارد)

سیستم انتقالی مساله شام خوردن فیلسوفان به کمک عملگر ترکیب موازی بصورت زیر بدست می آید

$$PHIL^i := LEFT^i \parallel_{\gamma} RIGHT^i$$

بگذارید

$$PHIL := PHIL^0 \parallel_{\gamma} PHIL^1 \parallel_{\gamma} PHIL^2 \parallel_{\gamma} PHIL^3 \parallel_{\gamma} PHIL^4$$

$$FORK := FORK^0 \parallel_{\gamma} FORK^1 \parallel_{\gamma} FORK^2 \parallel_{\gamma} FORK^3 \parallel_{\gamma} FORK^4$$

سیستم انتقالی مساله شام خوردن فیلسوفان عبارت است از

$$T := PHIL \parallel_{\gamma} FORK$$

دقت کنید در مساله بالا زمان بندی برای فیلسوفان در نظر نگرفتیم. پس در سیستم T می تواند مسیرهای ناموفقی باشد که هیچگاه یکی از فیلسوفها شام نخورد. باید بتوان این ویژگی را که آیا همه فیلسوفان شام می خورند را بصورت یک فرمول منطقی توصیف کرد. منطق زمانی این امکان را فراهم می سازد.

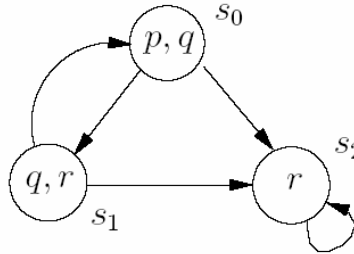
۲-۷ منطق LTL

منطق خطی زمانی¹¹⁵ LTL [؟] دارای ادات منطقی است که به آینده اشاره می‌کند. در این بخش به معرفی این منطق می‌پردازیم.

در بخش قبل، سیستم‌های انتقالی برچسب‌دار را معرفی کردیم. در این بخش نوعی دیگر از سیستم‌های انتقالی را در نظر می‌گیریم که به عنوان مدل‌های کرپسکی منطق زمانی در نظر گرفته می‌شوند.

تعریف ۲-۷-۱. فرض کنید P یک مجموعه از فرمول‌های اتمی باشد. یک سیستم انتقالی (مدل کرپسکی) روی P عبارت است چندتایی $M = \langle S, \rightarrow, V \rangle$ که S مجموعه‌ای از وضعیت‌ها، $\rightarrow \subseteq S \times S$ رابطه انتقال، و $V : S \rightarrow 2^P$ یک تابع ارزش‌دهی است.

مثال ۲-۷-۲. یک سیستم انتقالی روی مجموعه فرمول‌های اتمی $P = \{p, q, r\}$



تعریف ۲-۷-۳. (زبان منطق LTL). فرض کنید P یک مجموعه از فرمول‌های اتمی باشد. زبان

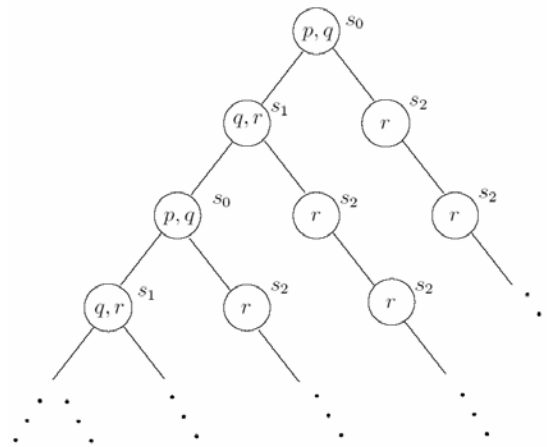
$L_T(P)$ کوچکترین مجموعه‌ای شامل P است بطوریکه

$$\varphi, \psi \in L_T(P) \Rightarrow \neg\varphi, (\varphi \wedge \psi), X\varphi, F\varphi, G\varphi, \varphi U \psi, \varphi W \psi, \varphi R \psi \in L_T(P)$$

تعریف ۴-۲-۷. یک مسیر از مدل کرپکی $M = \langle S, \rightarrow, V \rangle$ یک دنباله نامتناهی

$s_1, s_2, \dots, s_n \dots$ از وضعیتها است که برای هر i ، $(s_i, s_{i+1}) \in \rightarrow$. مجموعه مسیرهای ممکن M را با $path(M)$ نمایش می‌دهیم. برای مسیر $\pi = s_1 \rightarrow s_2 \rightarrow \dots$ و $k > 0$ ، π^k زیر مسیری از π است که از گام k ام آغاز می‌شود.

مثال ۵-۲-۷. شکل زیر مسیرهای ممکن سیستم انتقالی مثال ۲-۲-۷ را نمایش می‌دهد.



تعریف ۶-۲-۷. فرض کنید $M = \langle S, \rightarrow, V \rangle$ یک سیستم انتقالی و $\pi \in path(M)$ مسیر

$\pi = s_1 \rightarrow s_2 \rightarrow \dots$ فرمولهای منطق LTL را بصورت زیر ارضا می‌کند.

۱. برای فرمولهای اتمی $p \models \pi$ اگر و تنها اگر $p \in V(s_1)$

۲. $\pi \models \neg \varphi$ اگر و تنها اگر $\pi \not\models \varphi$

۳. $\pi \models \varphi \wedge \psi$ اگر و تنها اگر $\pi \models \varphi$ و $\pi \models \psi$

۴. $\pi^2 \models \varphi$ اگر و تنها اگر $\pi \models X\varphi$

۵. $\pi^k \models \varphi$ اگر و تنها اگر وجود داشته باشد $k \geq 1$ که $\pi \models F\varphi$.

۶. $\pi \models G\varphi$ اگر و تنها اگر برای هر $k \geq 1$ ، $\pi^k \models \varphi$ ($\pi \models G\varphi$) اگر و تنها اگر

$$(\pi \models \neg F\neg\varphi$$

۷. $\pi \models \varphi U \psi$ اگر و تنها اگر وجود داشته باشد $i \geq 1$ بطوریکه برای هر $1 \leq j < i$ ،

$$\pi^i \models \psi \text{ و } \pi^j \models \varphi$$

۸. $\pi \models \varphi W \psi$ اگر و تنها اگر یا $\pi \models G\varphi$ یا $\pi \models \varphi U \psi$ یا $\pi \models \varphi W \psi$ ($\pi \models \varphi W \psi$) اگر و تنها

$$\pi \models (\varphi U \psi) \vee G\varphi \text{ اگر}$$

۹. $\pi \models \varphi R \psi$ اگر و تنها اگر یا $\pi \models G\psi$ یا $\pi \models \psi U (\psi \wedge \varphi)$.

تعریف ۷-۲-۷. فرض کنید $M = \langle S, \rightarrow, V \rangle$ یک سیستم انتقالی باشد. برای $s \in S$ ،

$$(M, s) \models \varphi \text{ هرگاه برای هر مسیر } \pi \text{ که از } s \text{ آغاز شود داشته باشیم } \pi \models \varphi.$$

خواندن عملگرهای زمانی

عملگرهای زمانی را به صورت زیر بخوانید

$$(M, s) \models F\varphi: \text{ رویارویی با برقراری } \varphi \text{ در آینده } s, \text{ اجتناب ناپذیر است.}$$

$$(M, s) \models \varphi U \psi: \text{ رویارویی با برقراری } \psi \text{ در آینده } s, \text{ اجتناب ناپذیر است و در آینده } \varphi \text{ برقرار}$$

خواهد بود مادامیکه ψ برقرار شود.

$$(M, s) \models X\varphi: \text{ در وضعیت تالی } s, \varphi \text{ برقرار است.}$$

مثال ۷-۲-۸. سیستم انتقالی مثال ۷-۲-۲ را در نظر بگیرید. با توجه به شکل مثال ۷-۲-۵ داریم:

$$(M, s_0) \models Xr$$

$$(M, s_0) \models Fr$$

$$(M, s_0) \models qUr$$

تمرین. گوییم دو فرمول φ, ψ از منطق LTL معادل هستند ($\varphi \equiv \psi$)، هرگاه برای هر سیستم انتقالی $M = \langle S, \rightarrow, V \rangle$ و $s \in S$ داشته باشیم $(M, s) \models \varphi$ اگر و تنها اگر $(M, s) \models \psi$.

نشان دهید

$$F(\varphi \vee \psi) \equiv F\varphi \vee F\psi$$

$$\neg(\varphi U \psi) \equiv \neg\varphi R \neg\psi$$

.....

۷-۳ منطق CTL

.....

مراجع

- [1] M. Huth and M. Ryan, **Logic in Computer Science**
- [2] C. Bair, J. P. Katoen, **Principles of Model Checking**, MIT Press, 2008.
- [3] C.A. Middelburg, M.A. Reniers, **Introduction to Process Theory**, 2005.
- [4] W. Fokkink, **Introduction to Process Algebra**, 2007.

بخش سوم

ابزارهاي پياده سازي