بسم الله الرحمن الرحيم

وزارت علوم، تحقیقات و فناوری

دانشگاه پیام نور

امنیت روشهای ترکیب بهینه وب سرویس ها

مجری :

افسانه بنی طالبی دهکردی

تاریخ :

مهر ۱۳۹۵

تقدیم به :

پدرم

کوهی استوار و حامی من در طول تمام زندگی

مادرم

سنگ صبوری که الفبای زندگی به من آموخت

و

همسرم

اسطوره زندگیم، پناه خستگیم و امید بودنم.

و

گل نازم

آیسا

تشکر و قدردانی

اکنون که با لطف وعنایت پروردگار عزوجل این پژوهش به پایان رسیده است برخود لازم می دانم که بهترین سپاس خویش را به محضر مسئولین محترم دانشگاه پیام نورکه با ژرف نگری وصبر خویش همچنین حمایت های مادی و معنوی در حل مشکلات و اهتمام در پیشبرد این پژوهش مرا یاری نموده اند ، تشکر و قدردانی بنمایم .

چکیده

وب سرویسها اجزای نرم افزاری ماژولار، جامع، مستقل و قابل استفاده مجدد هستند که تعاملات تجاری را در محیط های توزیع شده آسان کرده اند.امروزه وب سرویس ها یکی از مهمترین گروه های مورد استفاده در معماری و محاسبات سرویس گرا هستند . وب سرویس نرم افزاری است که دسترسی به اطلاعات و نیز سیستم های پردازش اطلاعات را بصورت توزیع شده جداازپلتفرمهای سخت افزاری و با استفاده ازپروتکلهای استاندارد اطلاعات اینترنتی فراهم می کند درحال حاضرمسائل امنیتی بزرگترین مانع گسترش وب سرویس درسطح تشکیلات می باشد تلاشهایی درزمینه وب سرویسها انجام شده است که شامل ارایه استانداردها پروتکلها و تکنولوژیهای درزمینه برآورده نمودن نیازهای امنیتی وب سرویسها می باشد. گاهی اوقات برای انجام یک درخواست نمی توان از یک وب سرویس استفاده کرد و لازم است چندین سرویس یک درخواست را انجام دهند . به فرآیند ترکیب چند وب سرویس، وب سرویس مرکب گفته می شود. یکی از مسائل چالش برانگیز در ترکیب وب سرویس ها، انتخاب وب سرویس هاست .باتوجه به تعداد زیاد وب سرویس ها در محیط های توزیع شده انتخاب وب سرویس ها نقش مهمی را در ترکیب وب سرویس ها بازی می کند .وب سرویس هایی که برای انجام یک کار کاندید می شوند از نظر خصوصیات عملیاتی یکسان هستند یعنی همگی کار موردنظر را انجام می دهند؛ اما از نظر خصوصیات کیفی با هم متفاوت هستند .بنابراین انتخاب وب سرویس براساس ویژگی های کیفی یک مسأله مهم و قابل توجه در سیستم های توزیع شده است. کاربران تمایل دارند وب سرویسی را انتخاب کنند که نیازمندیهایشان را برآورده کند .در این طرح پژوهشی برروی راهکار انتخاب وب سرویس ها براساس ویژگی های کیفی وامنیت وب سرویس هابا استفاده از تکنیک Apache Rampart تمرکز شده است و یک روش جدید برای ترکیب و انتخاب وب سرویس ها با استفاده از روش های هوش مصنوعی مانند آتوماتای سلولی ارائه خواهدشد.

یک آتوماتای سلولی یک ماشین محاسباتی است که متشکل از دو بخش فضای سلولی و قانون انتقال محلی است که هر سلول می تواند حالتهای مختلفی داشته باشد که با اندیس i مشخص می شود و حالت هر سلول در زمان t نشان داده می شود. هر سلول دارای همسایگانی است که با استفاده از آنها می توان قانون انتقال محلی را اعمال کرد و مجموعه حالت همسایگان سلول i در زمان t مشخص می شود و شعاع همسایگی هر سلول با r مشخص می شود. هر اتوماتای سلولی بصورت یک چهارتایی شامل

$CA = (\sum , d , V, \Phi)$

می باشد که داریم :

$\sum$: مجموعه وضعیتهای ممکن یک سلول

D : بعد اتوماتای سلولی

V : ساختار همسایگی اتوماتای سلولی

Φ : قانون انتقال محلی

فهرست مطالب

فهرست نمودارها

فهرست شکل ها

فصل اول

کلیات پژوهش

۱-۱ وب سرویس[۱]

وب سرویس ها برنامه یا قطعه کدهایی هستند که تحت وب قابل دسترسی اند و از طریق پروتکل های استانداردی مانند Http به انتقال و مبادله دیتا با سایر برنامه های کاربردی می پردازند. اساس کار وب سرویس ها بر پایه دریافت و تولید پیغام بنیان گذاری شده است. بدین معنی که آنها منتظر می مانند که کلاینت ها به آنها وصل شده و بنا به درخواست کلاینت ها به آن ها پاسخ می دهند .وب سرویسها می توانند application ها را به Web-Application تبدیل کنند، که در این صورت کارکردهای آنها در سطح جهانی گسترش پیدا خواهد کرد. وب سرویسها اجزای یک نرم افزار هستند. آنها از طریق پروتکل ارتباط برقرار می کنندو منابع بیرونی نداشته و اصطلاحا self-contained هستند.وب سرویسها از طریق UDDI قابل جستجو هستندوتوسط application های دیگر قابل استفاده اند[۱].

۱-۲ ویژگی های کلی وب سرویس ها

- وب سرویس ها به سیستم عامل و زبان برنامه نویسی وابستگی ندارند
- فراخوانی یک وب سرویس توسط برنامه ها مستقل از سیستم عامل و زبان برنامه نویسی به کار رفته می باشد.
- سهولت در برقراری ارتباط بین برنامه ها
- انتقال اطلاعات بین برنامه ها از طریق وب سرویس بسیار آسان صورت می پذیرد.
- استفاده مجدد از کامپوننت های نرم افزاری
- اتصال به نرم افزارهای موجود
- وب سرویسها می توانند با یک متد مشخص داده ها و اطلاعات application های مختلف را به هم پیوند داده و از این طریق مشکلات موجود در این همکاری ها را مرتفع کنند[۱].

[۱] Web Service

شکل ۱-۱ : وب سرویس

۱-۳ پروتوکل های استاندارد مورد استفاده وب سرویسها

استانداردهای مختلفی مورد استفاده وب سرویس ها است که درادامه به معرفی آنها می پردازیم[۲]:

- XML (eXtensible Markup Languag)

تکنولوژی XML در سال ۱۹۹۶ توسط کنسرسیوم W۳C ایجاد و استاندارد شده است. فایل های XML حاوی اطلاعات و دیتا در قالب متن و فاقد شکل و ظاهر می باشند و تنها برای انتقال و مبادله داده ها بین وب سرویس ها و برنامه ها به کار می روند. چنانچه XML برای برنامه ای قابل شناسایی باشد برنامه مورد نظر می تواند بدون آنکه نیاز به برنامه و سیستم عامل خاصی داشته باشد به اطلاعات درون فایل xml دسترسی پیدا کند .

- SOAP (Simple Object Access Protocol)

استاندارد مهم دیگری که در وب سرویس ها به کار می رود استاندارد SOAP است. این استاندارد عامل ایجاد ارتباط بین نرم افزارها یا برنامه های کاربردی و وب سرویس می باشد این ارتباط اغلب از طریق پروتکل امن Http صورت می پذیرد. هنگامی که یک برنامه اقدام به ارتباط با یک وب سرویس می نماید پیغام های SOAP عامل ایجاد ارتباط و انتقال اطلاعات بین آن دو می باشند، یک پیغام SOAP که حاوی درخواست فراخوانی و اجرای یک تابع (در وب سرویس) می باشد به Web Service ارسال می شود پیغام ارسال شده توسط وب سرویس بررسی شده و سپس به اجرای درخواست (اجرای تابع) می پردازد و نهایتا نتیجه را در قالب یک پیغام SOAP به برنامه اصلی می فرستد.

- WSDL (Web Service Description Language)

یکی از استانداردهای مهم در وب سرویس ها استاندارد WSDL است. هر وب سرویس دارای یک فایل WSDL می باشد. این فایل به توصیف وب سرویس می پردازد و نحوه استفاده از وب سرویس را توضیح می دهد و به صورت یک فایل متنی با فرمت XML می باشد که به برنامه ها می گوید که وب سرویس مورد نظر چه ورودی هایی دریافت و چه خروجی هایی را به برنامه

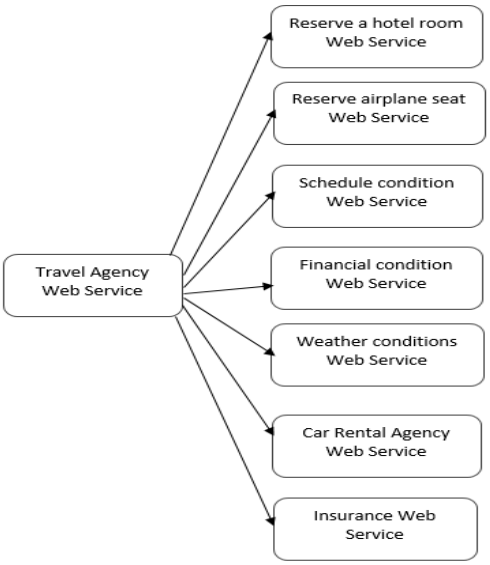
برمی گرداند WSDL صرفا برای برنامه طراحی شده است نه برای کاربران استفاده کننده از وب سرویس. بسیاری از نرم افزارهایی که به ساخت وب سرویس می پردازند فایل WSDL وب سرویس را نیز خود به صورت اتوماتیک تولید می کنند.

- UDDI (Universal Description Discovery and Integration)

از طریق این استاندارد، ثبت و جستجوی وب سرویس ها در اینترنت فراهم می گردد. این استاندارد توسط شرکت مایکروسافت، IBM و شرکت های بزرگ دیگر تولید شده است. با استفاده از این استاندارد شرکت ها قادرند به مبادله اطلاعات با سایر شرکت ها پرداخته و مدل B۲B ایجاد نمایند. UDDI یک فایل مبتنی بر XML می باشد که در آن شرکت ها به معرفی امکانات وب سرویس خود و نحوه عملکرد آن می پردازند. همچنین شرکت ها می توانند اجازه دستیابی به این فایل را تنها به شرکت های خاصی بدهند و یا اینکه آنها را به صورت عمومی در اینترنت قرار دهند.

- **۱-۴ روشهای ترکیب بهینه سرویسهای وب بر اساس کیفیت آنها**

برای انجام یک کار ممکن است نیاز به انواع سرویس های مختلفی باشد که در کنار هم یک وب سرویس مرکب را تشکیل داده تا هدف مورد نظر را تامین کنند[۳].برای مثال یک آژانش هواپیمایی برای انجام یک خدمت نیاز به رزرو بلیط هواپیما ، برنامه ریزی شرایط ، برنامه ریزی مالی ، بررسی وضعیت آب و هوا ، رزرو ماشین و ارائه خدمات بیمه دارد. این خدمات در کنار هم برای ارائه یک خدمت آژانس های مسافرتی نیاز است. حال می توان برای هرکدام ازاین کارها یک وب سرویس ارائه داد تا این کار را انجام دهد. شکل ۱-۲ به بیان این وب سرویس ها می پردازد.



شکل ۱-۲ : وب سرویس خدمات مسافرتی

فرایند پیدا کردن ترکیب سرویسهای مناسب بر اساس درخواست کاربر دارای سه مرحله می باشد[۴].

۱) ایجاد مدل کیفیت سرویس مناسب
۲) کشف و انتخاب وب سرویس های مناسب
۳) ایجاد ترکیب مناسب بر اساس وب سرویسهای انتخاب شده

- **مدل کیفیت سرویس**

اولین مرحله برای بدست آوردن ترکیب بهینه وب سرویسها ایجاد یک مدل مناسب برای توصیف ویژگی های کیفی آنها می باشد. این مدل باید مورد توافق مشتری و فراهم کننده سرویس باشد. ویژگی های کیفی وب سرویسها به دو دسته کلی ، ویژگیهای مثبت و ویژگی های منفی تقسیم می شود . مهمترین این ویژگی ها عبارتند از زمان پاسخ ، هزینه ، قابلیت اطمینان و قابلیت دسترسی . از جمله موارد دیگری که باید در مدل کیفیت سرویس مشخص شود چگونگی محاسبه مقدار مجموع ویژگی های کیفی وب سرویس مرکب می باشد.

- **کشف و انتخاب وب سرویسهای مناسب**

بعد از ایجاد مدل کیفیت سرویس مورد نظر، نوبت به کشف وب سرویس های مناسب می رسد. انتخاب وب سرویس یک روند دو مرحله ای است: در مرحله اول که تطابق عملیاتی نامیده می شود وب سرویس هایی که عملکرد آنها باعملکرد مورد نظر مشتری مطابقت دارد انتخاب می شوند . استاندارد UDDIاین امکان را دارد که وب سرویس های مورد نظر را جستجو کند . در مرحله دوم که تطابق غیر عملیاتی نامیده می شود وب سرویس هایی که کیفیت عملکردآنها مناسب باشند ، انتخاب می شود.

- **بدست آوردن ترکیب بهینه وب سرویسها بر اساس کیفیت سرویس**

تاکنون روشهای مختلفی برای حل مسأله ترکیب وب سرویسها براساس ویژگیهای کیفی پیشنهاد شده است که می توان این روشها را به دو دسته کلی متدهای دقیق یا همان غیر ابتکاری و متدهای تقریبی یا در واقع ابتکاری تقسیم بندی نمود[۵].

- **روشهای غیر ابتکاری**

این دسته روشهایی هستند که برای انتخاب بهترین طرح از میان طرحهای موجود تمام مسیرهای کاندید را بررسی و محاسبه می کنند و در نتیجه ما را به جواب دقیق تری می رسانند. سودمندی با در نظر گرفتن محدودیتها می باشد. این محدودیتها در واقع همان نیازمندیهای کیفی مورد نظر مشتریان مانند زمان پاسخ، هزینه، قابلیت اطمینان و قابلیت دسترسی هستند که باید مطابق با خواسته کاربر در نظر گرفته شوند. آنها الگوریتم خود را براساس مدل ترتیبی بنا نهاده و تنها یک محدودیت را در نظر گرفته اند.آنها دو روش متفاوت برای حل مسأله ارائه کرده اند.

  - **روش اول مسأله به عنوان یک مسأله کوله پشتی**

دراین مسأله هر آیتم یک وزن و یک سودمندی دارد و خود کوله پشتی هم یک گنجایش مشخصی دارد. هر کدام از آیتم ها در واقع یک سرویس کاندید هستند که سودمندی و وزن آنها به ترتیب همان ارزش و ویژگیهای کیفی سرویس را نشان می دهد. گنجایش کوله پشتی یک محدودیت سراسری می باشد. الگوریتم برای انتخاب یک سرویس از مجموع سرویسهای کاندید تلاش می کند، بطوریکه ارزش مجموع سرویسها با شرط در نظر گرفتن گنجایش کوله پشتی ماکزیمم شود.

این مسأله بصورت فرمول (۱-۱) بیان شده است. آنها برای حل مسأله از روش برنامه نویسی پویا استفاده کردند

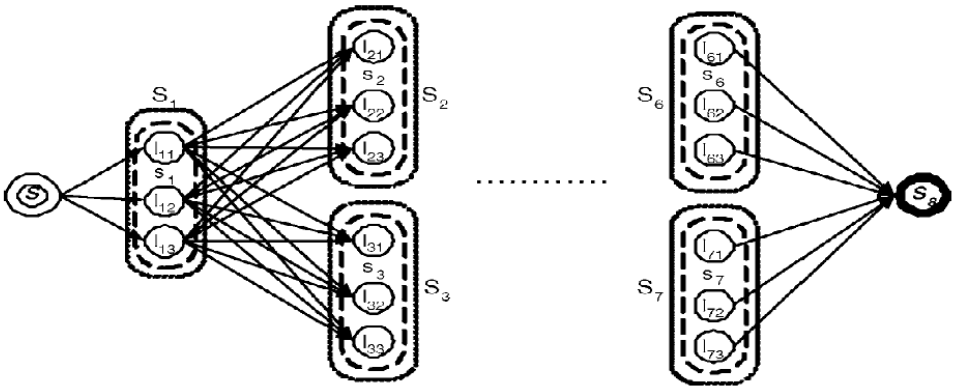
فرمول ۱-۱

$$Max \sum_{i=1}^{k} \sum_{j \in s_i} F_{ij} x_{ij}$$

$$Subject\ to \sum_{i=1}^{k} \sum_{j \in s_i} R_{ij} x_{ij} \leq R$$

$$, \sum x_{ij} = 1$$

روش دوم این تحقیق یک تئوری گراف است بطور کلی ایده اصلی در این تئوری این است که مسأله بصورت یک مسأله یافتن کوتاهترین مسیر در گراف در آورده شود. در این روش هر سرویس کاندید به صورت یک نود نشان داده شده است. یالها ارتباط میان سرویسها را بیان می کنند. هزینه یالها در واقع همان ویژگیهای کیفی هستند در اینجا هزینه و تأخیرگراف مورد نظر در شکل ۱-۳ نشان داده شده است.



شکل ۱-۳ : تشکیل گراف وب سرویس ها برای حل مساله ترکیب وب سرویس

حال باید کوتاهترین مسیر بین فرآیند S وفرایند S۸ را درکمترین زمان پیدا کرد به طوریکه مجموع وزن یالها از آنچه مورد نظر کاربر است بیشتر نشود. برای یافتن مسیردو روش CBF[۲] و CSP[۳] ارائه و مقایسه شده است. نتایج نشان می دهد که روشCSP کارآیی بیشتر و زمان اجرای کمتری نسبت به CBF دارد.

[۲] Constrained Bellman Ford
[۳] Constrained Shortest Path

از دیگر روشهای دسته اول در حل این مسأله روش برنامه ریزی خطی می باشد که برای حل مسائلی که تابع هدف خطی دارند کاربرد دارد. برنامه ریزی خطی سعی بر آن دارد تا از طریق تنظیم مقادیر متغیرها مقدار تابع را بیشینه یا کمینه کند.
تحقیقات نشان داده است که برای محیطهای کوچک و ساده با تعداد کم وب سرویسهای کاندید روشهای گروه اول مناسب می باشند ولی با افزایش تعداد وب سرویسها و بزرگ تر و پیچیده تر شدن محیط، به علت عدم مقیاس پذیری، افزایش نمایی زمان اجرا و پیچیدگی روش های غیرابتکاری، متدهای گروه دوم که شامل الگوریتمهایی با سرعت بالاتر و پیچیدگی کمتری می باشند مناسب تر هستند و می توانند بهترین راه حلها را درزمانی قابل قبول پیدا کنند

- **روش های ابتکاری**

این الگوریتمها روشهایی هستند که بر پایه الهام گرفتن از پدیده های طبیعی، زیستی یا اجتماعی کار خود را انجام می دهند[۶]. مزایایی چون مقیاس پذیری، تطابق پذیری، قابلیت اطمینان و زمان اجرای قابل قبول باعث شده تا انواع مختلفی از این الگوریتمها از جمله الگوریتم ژنتیک، کلونی مورچگان، تجمع ذرات یا همان جمعیت پرندگان، رقابت استعماری و... را تبدیل به روشهایی نیرومند در حل مسائل بهینه سازی و به طبع مسأله بهینه سازی ترکیب وب سرویسها کند.
دراین پژوهش روش آتاماتای سلولی که یکی از روشهای ابتکاری است برای ترکیب وب سرویس ها بکار رفته است. درفصل دوم به معرفی این روش و مطالعات انجام شده دراین حوزه پرداخته و یک بسته امنیتی برای بالا بردن امنیت مبتنی بر روش Apache Rampart بیان می کنیم.

فصل دوم

مروری بر مطالعات انجام شده (پیشینه پژوهش)

دراین فصل به معرفی آتاماتای سلولی که یکی از روشهای ابتکاری برای ترکیب وب سرویس ها است پرداخته شده و مطالعات انجام شده دراین حوزه را مورد بررسی قرار می دهیم[۷].

۲-۱ ماهیت آتوماتای سلولی

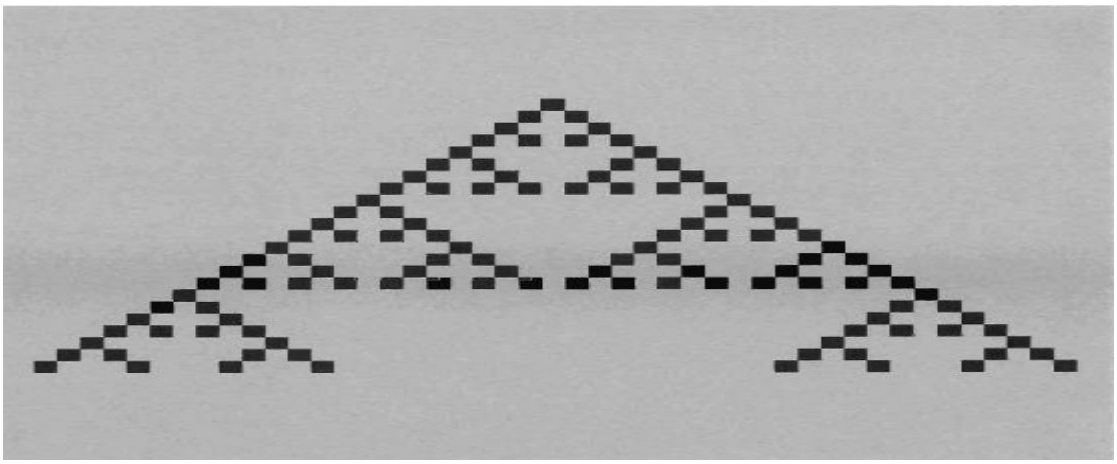
آتوماتای سلولی، ایده آل سازی های ساده ریاضی از سیستم های طبیعی هستند. آنها شامل شبکه ای از مکـان هـای مشـابه و مجزایی هستند هر قسمت نیز دارای مجموعه ای متناهی از مقادیر صحیح می باشد. مقادیر قسمتها در مراحل زمانی مجزا ظاهر می شوند.آتوماتای سلولی ممکن است به عنوان ایده آل سازه های مجزای معادلات دیفرانسیلی جزئی در نظـر گرفتـه شـوند و اغلـب سیستم های طبیعی را توضیح می دهند. علاوه بر این، ماهیت مجزای آنها امکان یک مقیاس مهم را با رایانه های دیجیتـالی فـراهم می کند: ممکن است آتوماتای های سلولی به عنوان رایانه های شبه پردازش با طرح ساده بررسی شوند.

به عنوان مثال اول از یک آتوماتای سلولی خطی از مکان ها را در نظر بگیرید(هر کدام دارای مقادیر صفر یا یک هستند)مقدار یک مکان را در موقعیت روبروی مرحله زمانیt، ai در نظر بگیرید. یک قانون بسیار ساده برای تکامل زمانی این مقادیر مکانی عبارتست از:[۸]

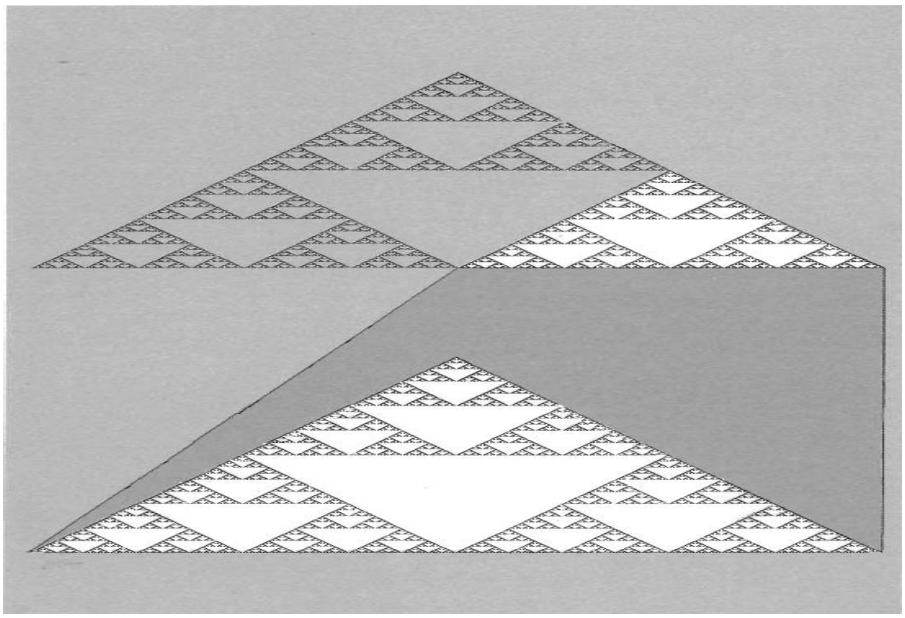
$$ai(t+۱)= ai-۱(t)+ ai+۱(t) \bmod ۲ \qquad \text{(معادله ۲-۱)}$$

در اینجا x مد۲ نشان می دهد که باقیمانده صفر یا یک پس از تقسیم شدن بوسیله ۲ بدست می آید. طبق این قانون مقدار یک مکان ویژه بوسیله مجموع مدولوی۲ از مقادیرنزدیکترین مکان مجاور چپ و راست (بر روی مرحله زمان قبلی) داده می شود. قانون به طور همزمان در هر مکان اجرا می شود حتی با این قانون بسیار ساده عملکردی کاملا پیچیده یافت می شود.

شکل ۲-۱ : نحوه تبدیل عدد در مبنای ۲ به فرمتی برای نمایش



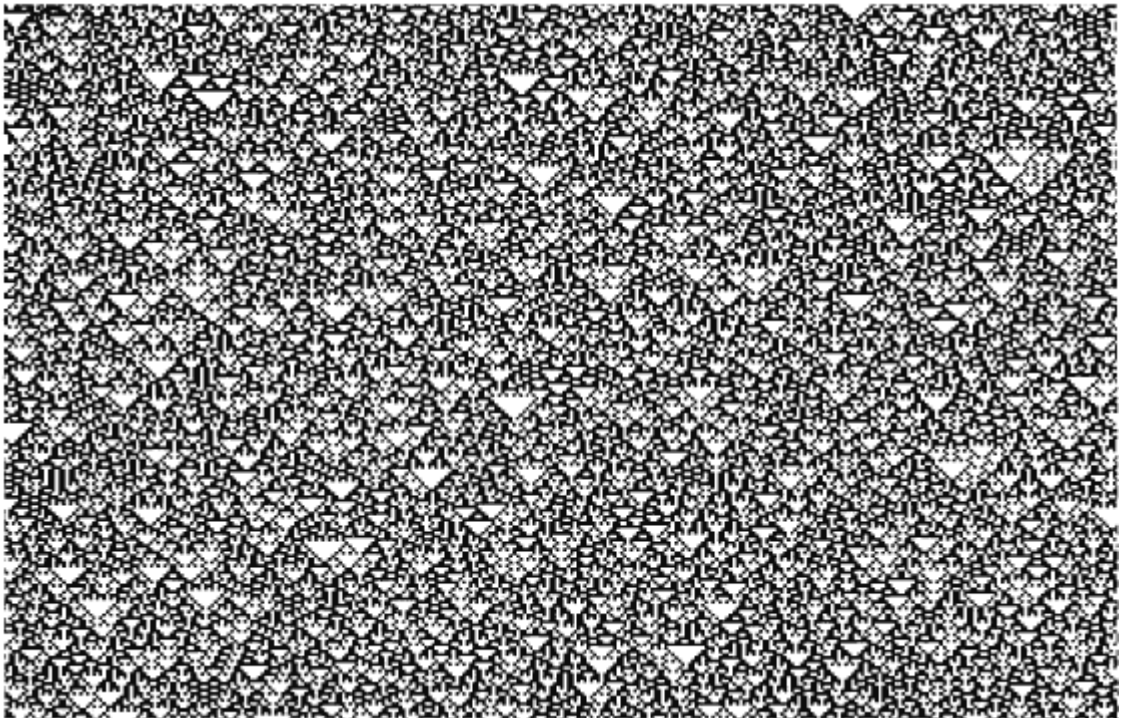
شکل۲-۲: شکل حاصل از اعمال معادله ۱ در آتاماتای سلولی ساده



شکل ۲-۳: شکل حاصل از توسعه معادله ۱ از آتوماتای سلولی ساده به تعداد ۵۰۰ مرتبه

نمونه های کسری از آتوماتای سلولی حاصل می شوند. اول از همه،طبق معادله اول، تکامل را در نظر بگیرید. هر دانه شامل مکان منفردی با مقدار یک است. دیگر مکان ها دارای مقدار صفر هستند.نمونه یا الگوی مذکوربرای تعدادی از مراحل زمانی بوسیله تکامل ایجاد می شود هم اکنون نیز،تعدادی ساختار را نشان می دهد. تصویر شماره ۲-۳، نمونه ای را پس از ۵۰۰ مرحله زمانی نشان می دهد. تشکیل این الگو مستلزم کاربرد معادله در یک چهارم از یک میلیون مقادیر مکانی می باشد. الگوی تصاویر ۲-۳ و۲-۲ ،نمونه پیچیده ای است. اما نظم و تربیت های چشمگیری را نشان می دهد. یکی از آنها،خود تشابهی است. همان طور که

در تصویر شماره۲-۳، نشان داده شده قسمتهایی از این الگو در حین بزرگ شدن ،از کل الگو،قابل تشخیص نیستند. بنابراین الگوی مذکور،تحت درجه بندی مجدد طول ها،ثابت می ماند. اغلب،چنین الگوی خود مشابهی را یک کسر (فراکتال)می نامند. و ممکن است بوسیله یک بعد کسری مشخص میشود.بسیاری از سیستم های طبیعی مانند دانه های برف،نشان دهنده نمونه های کسری هستند. بسیارمحتمل است که در بسیاری از موارد این نمونه های کسری از طریق تکامل آتوماتای ها یا فرآیند های قابل قیاس،به وجود می آیند.



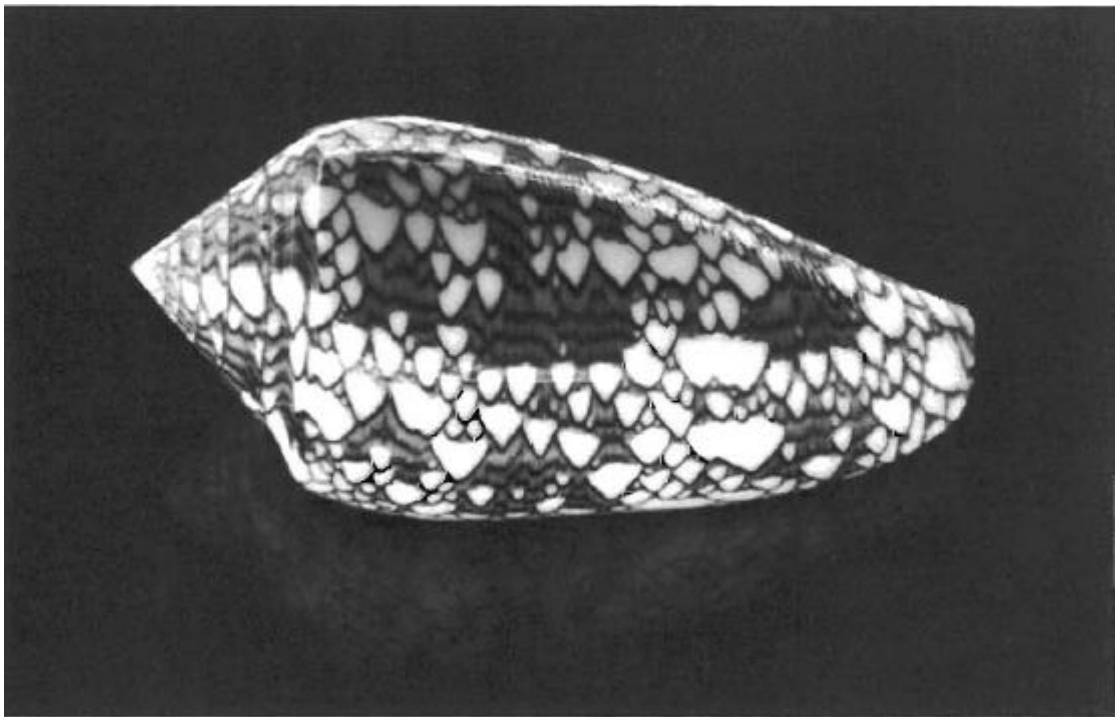
شکل۲-۴: شکل حاصل از تکامل معادله ۲-۱در آتوماتای سلولی ساده

۲-۲ خود سازمانی در آتوماتای سلولی

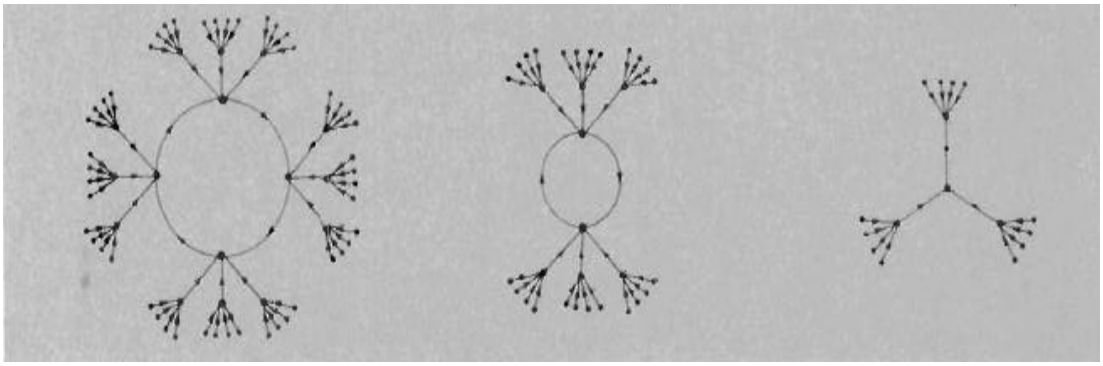
تصویر۲-۴ نشان دهنده تکامل می باشد(طبق معادله آن از حالت اولیه بی نظمی). مقادیر مکان ها در این حالت اولیه به ندرت انتخاب می شوند:هر مکان مقدار صفر یا یک را با احتمال مساوی انتخاب می کند(جدای از مقادیر مکان های دیگر) با وجود آنکه حالت اولیه،ساختار ندارد،اما تکامل آتوماتای سلولی،نشان دهنده بعضی از ساختارها در فرم تسویه های مثلثی می باشد. ظهورخود به خود این تسویه ها،نمونه ساده ای است از خود سازماندهی .نمونه تصویرها،بیانگر نمونه رنگ یافت شده در پوست فرم تنان ویژه می باشد. کاملا امکان پذیر است که رشد این نمونه های رنگی،دنبال کننده قوانین آتوماتای سلولی باشد.

در سیستم هایی که ترمودینامیک معمولی را دنبال می کنند،قانون دوم ترمودینامیک نشان دهنده انحطاط و تجزیه پیشرفته در ساختار اولیه و نیز تمایل عمومی و کلی نسبت به تکمیل شدن یا زمان و رسیدن به حالات نظیر ماکسیمم آنتروپی وبی نظمی می باشد. در حالیکه بسیاری از سیستم های طبیعی تمایل به بی نظمی دارند(گروه بزرگی از سیستم ها) اما انواع بیولوژیک ،نمونه های اولیه هستند که روند معکوسی را نشان می دهند: آنها به طور خود به خود ،ساختاری را با زمان ایجاد می کنند(حتی زمانیکه از حالات اولیه نا منظم یا بدون ساختار آغاز می شوند)[۹]. آتوماتای سلولی در تصویر ۲-۵،نمونه ای ساده از چنین سیستم خود سازمان یافته ای می باشد. اساس و معیار ریاضی این عملکرد بوسیله بررسی ویژگی ها کلی آتوماتای سلولی آشکار می شود. به جای دنبال کردن تکامل از حالت اولیه ویژه(تصویر ۲-۵) می توان تکامل کلی یک مجموعه کامل را در بسیاری از حالات اولیه مختلف دنبال کرد.

بررسی ویژگی های کلی و آتوماتای سلولی متناهی که شامل تعداد محدودی از سایتها و مکان ها می شوند آسان تر است مکان های مذکور در معرض شرایط حدی ادواری قرار دارند. چنین آتوماتای سلولی محدود ممکن است به عنوان مکان های مرتب شده نشان داده شود (اطراف یک دایره)اگر هر مکان دو مقدار اولیه داشته باشد(همان گونه که برای قانون معادله اول نیز دلالت دارد)در آن صورت برای تکمیل شدن آتوماتای سلولی محدود،حالات کلی احتمالی ۲ به توان n وجود خواهد داشت. سپس،ممکن است، تکامل کلی آتوماتای سلولی بوسیله گراف انتقالی حالت اولیه نشان داده شود.



شکل ۲-۵: صدف شیپوری با پوسته ای که نقش روی آن بوسیله آتوماتای سلولی ایجاد شده



شکل ۲-۶ : گراف عمومی انتقال حالت برای آتوماتای سلولی متناهی

گراف مذکور درفضای حالت از اتومانون سلولی ترسیم می شود. هر حالت احتمالی ۲ به توان n از آتوماتای کامل سلولی بوسیله یک گره یا نقطه (در گراف)ایجاد می شود. و یک خط مستقیم هر گره را به گره ایجاد شده،متصل می کند(بوسیله کاربرد منفرد قانون آتوماتای سلولی)مسیر،در حالت بوسیله خطوط مستقیم متصل کننده یک گره ویژه به جانشین هایش ترسیم می شود.

بنابراین با تکامل زمانی آتوماتای سلولی حالت اولیه مطابقت می کند و بوسیله یک گره ویژه نشان داده مـی شـود. گـراف انتقـال حالت در تصویر ۲-۶، نشان دهنده همه مسیرهای احتمالی در حالت برای یک آتوماتای سلولی با دوازده مکان می باشـد و طبـق قانون ساده معادله۲-۱،تکمیل می شود.

ویژگی چشمگیر تصویر ۲-۶،همان وجود مسیرهایی است که بازمان از بین می رونـد.در حالیکـه هـر مکـان دارای یـک جانشـین منحصر به فرد در زمان است. اما ممکن است چندین نمونه اولیه داشته باشد یا اینکه اصلا دارای نمونه اولیه نباشد. نا پدیـد شـدن مسیرها بیانگر آنست که اطلاعات در تکامل آتوماتای سلولی از بین می رونـد:اطلاعات و معلومـات حالـت از یـک سیسـتم و در زمانی ویژه بدست می آید،اما صرفا برای تعیین تاریخچه کافی نیست،به طوری که تکامل غیر قابل برگشت می شود. با آغـاز یـک مجموعه کلی اولیـه کـه در آن همـه ترکیبـات بـا توزیـع احتمـالات رخ مـی دهنـد،تکامل غیـر قابـل برگشـت،برای یـک سـری ترکیبات،احتمالات را کاهش داده و برای سری دیگرآنهـا را افـزایش مـی دهـد. مـثلا،پس از یـک مرحلـه زمانی،احتمـالات بـرای حالتهایی در اطراف گراف انتقالی حالت در تصویر ۲-۶،به صفر کاهش می یابد:ممکن است چنین حالتهایی به عنوان شرایط اولیـه داده شوند،اما ممکن است هیچ گاه از طریق تکامل آتوماتای سلولی بوجود نیایند. پس از تعداد زیـادی مرحلـه زمانی،تنهـا تعـداد محدودی از همه ترکیبات احتمالی رخ می دهد. آنهایی که رخ می دهند،ممکن است بر روی جذب کننده ها در تکامـل آتوماتـای سلولی قرار گیرند. علاوه بر این اگر حالتهای جذب کننده دارای ویژگی- های سازمان یافته ویژه ای باشند،این مشخصه ها به طور خود به خود در تکامل آتوماتای سلولی ظاهر می شوند. بنابراین احتمـال خـود سـازمان دهـی نتیجـه برگشـت ناپـذیری تکامـل آتوماتای سلولی می باشد،و ساختارها نیزاز طریق خود سازمان دهی بدست می آیند و بوسیله ویژگی های جذب کننده ها تعیـین می شوند.

برگشت ناپذیری تکامل آتوماتای سلولی بوسیله تصویر ۲-۶ نشان داده شده و در مقابل برگشت ناپذیری ذاتی سیستم هـایی مـی باشند مه بوسیله ترمودینامیک معمولی و موسوم توضیح داده می شوند. در یک سطح میکروسکوپی ،مسیرها نشـان دهنـده تکامـل حالتها در چنین سیستم هایی هستند که هیچ گاه از بین نمی روند:هر حالت دارای یک نمونه اولیه منحصر بـه فـرد اسـت. و هـیچ اطلاعاتی با زمان از بین نمی رود. از این رو،یک مجموعه کلی نا منظم که درآن همه حالات احتمالی با احتمالات مساوی رخ مـی

دهند. برای همیشه نا منظم باقی می مانند. علاوه بر این،اگر حالتهای مجاور گروه بندی شوند(بوسیله اندازه گیری های نادرست)[۱۰].

در آن صورت باگذر زمان احتمالات برای گروه های مختلف برابر می شوند(بدون توجه به مقادیر اولیه شان). در این روش،چنین سیستم هایی تمایل دارند که با گذر زمان بی نظمی خود را تکمیل کرده و به ماکسیمم آنتروپی برسند(طبق توضیح قانون دوم ترمودینامیک)تمایل به بی نظمی و افزایش آنتروپی،مشخصه هایی کلی از سیستم های برگشت پذیر هستند (در مکانیک آماری)سیستم های برگشت نا پذیر نظیر آتوماتای سلولی تصاویر ۲-۵و۲-۳و۲-۲،در مقابل این روند هستند اما هنوز هم قوانین کلی برای عملکرد و ساختارشان ایجاد شده و یافت می شوند. انتظار می رودکه این قوانین کلی در نهایت از بررسی نمونه های ساده قابل قیاس (ایجاد شده بوسیله آتوماتای سلولی)خود را جدا کنند.

در حالیکه مدارک و شواهدی مبنی بر اینکه قوانین اساسی میکروسکوپی فیزیک،به طور ذاتی برگشت پذیرند،وجود دارد اما بسیاری از سیستم ها به طور برگشت ناپذیری بر روی یک مقیاس ماکروسکپی عمل می کنند و بوسیله قوانین برگشت ناپذیر توضیح داده می شوند. مثلا در حالیکه تقابلات ملکولی میکروسکپی در یک سال سیال به طور کامل برگشت پذیرند،اما توضیحات ماکروسکپی مربوط به میانگین سرعت میدان در سیال با استفاده از معادلات نا ویرراستوکس برگشت نا پذیر نمی شوند و عبارات پخش کننده را در بر می گیرند. آتوماتای سلولی،مدل های ریاضی را در این سطح ماکروسکپی ارائه می دهند.

۲-۳ آنالیز ریاضی یک آتوماتای سلولی ساده

قانون آتوماتای سلولی معادله ۲-۱،ساده است و یک آنالیز ریاضی کامل را می پذیرد. نمونه های کسری تصاویر۲-۳ و۲-۲ ،در یک حالت ساده جبری مشخص می شوند. اگر هیچ مدولوی ۲ کاهشی،اجرا نشود،در آن صورت مقادیر مکان های ایجاد شده را از یک مکان اولیه غیر صفر،به سادگی به انتگرال ها تبدیل می شود و بدین طریق در مثلث پاسکال از ضرایب باینامیال ظاهر می شود. بنابراین نمونه مکان های غیر صفر در تصاویر ۲-۳ و۲-۲،همان نمونه ضرایب کسردار باینامیال در مثلث پاسکال می باشد.

برای تعیین ساختار نمودار انتقال حالت در تصویر ۲-۶،این روش جبری را می توان بسط و گسترش داد. بوسیله نوشتن هر ترکیب از پلی نامیال زیر،هر آنالیز ادامه می یابد:[۱۱]

$$A(x) = \sum_{i=0}^{N-1} a_i x^i$$ (معادله ۲–۲)

در اینجا x،یک متغیر مصنوعی است و ضریب xi ،مقدار مکان در موقعیت i می باشد. در عبارات پلی نامیال ها،قانون آتوماتای سلولی معادله ۱،فرم ساده ای را به خود می گیرد:[۱۱]

$$A(t+1)(x) = T(x)\ A(t)(x) \bmod(xn-1)$$ (معادله ۲–۳)

جایی که[۱]

$$T(x) = (x + x-1)$$ (معادله ۲–۴)

و همه حساب و اعداد بر روی ضرایب پلی نامیال مدولوی ۲ را اجرا می کند. مدولوی کاهش xn-۱ شرایط حدی ادواری را اجرا می کند. ساختار نمودار انتقال حالت از ویژگی های جبری نامیال T(x) استنباط می شود. حتی برای N مثلا می توان مشخص کرد که کسر حالات در جذب کننده ها، ۲-D(N) می باشد،در اینجا D۲(N) به عنوان بزرگترین نیروی انتگرال ۲ تعریف می شود که N را تقسیم می کند.

از آنجا که یک آتوماتای سلولی متناهی (محدود)به طور جبری با تعداد معینی حالت احتمالی تکمیل می شود می بایست در نهایت یک سیکل را وارد کرد به طوریکه یک سری حالت را به طور کلی ببیند و با آنها برخورد کند. این سیکل ها،به صورت حلقه های بسته در گراف انتقال حالت نمایان می شوند. آنالیز جبری مارتین نشان می دهد که برای آتوماتای سلولی معادله ۱ماکسیمم طول سیکل II حتی برای N به صورت زیر نیزداده می شود:[۱۱]

$$\Pi_{N=2^j} = 1$$ (معادله ۲–۵)

$$\Pi_{N=2(2k+1)} = 2\Pi_{N=2k+1}$$ (معادله ۲–۶)

برای کسر N، Π می تواند مورد زیر را تقسیم کند:[۱۱]

$$۲^{sord}N^{(۲)}-۱$$ (معادله ۲–۷)

و در حقیقت همواره با این مقدار برابر است. در اینجا$Sord\ N(۲)$ یک عد از تابع نظری است وبـرای $J=\pm ۱\ modulo\ N$ ۲ بـه صورت مینیمم عدد صحیح مثبت تعریف می شود. ماکسیمم مقدار $Sord\ N(۲)$،زمانی بدست می آید که N سلول و $(N-۱)/۲$ باشد. بنابراین ماکسیمم طول سیکل دارای درجه $N/۲$ ۲ است. و به طور تقریبی ریشه مربع عـدد کلـی حـالات احتمـالی $N۲$ مـی باشد.

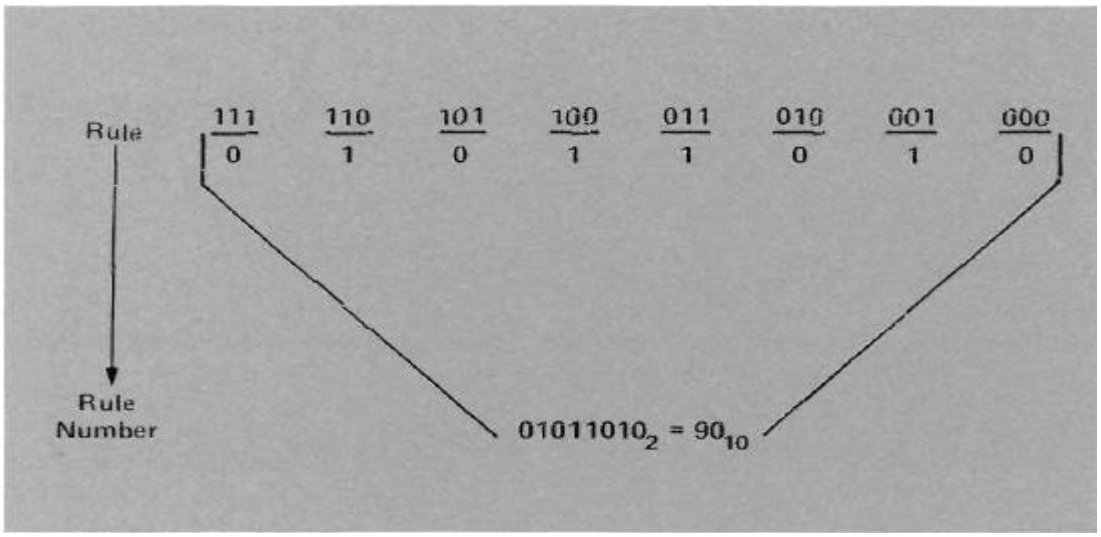
یک مشخصه نامعمول از این آنالیز ظهور تعدادی از مفاهیم نظری می باشد. تئوری یا نظریه اعداد با نتـایج پیچیـده منسـوخ شـده است (براساس فرضیات بسیار ساده)و ممکن است بخشی از مکانیسم ریاضـی باشـد کـه بوسـیله آن سیسـتم هـای طبیعـی طـرح ساده،عملکرد پیچیده ای را به وجود می آورند.

۲-۴ آتوماتای سلولی کلی

بحث مذکور تا کنون بر قانون آتوماتای سلولی ویژه(معادله ۲-۱)تاکید کرده است. این قانون می تواند به چنـین روش تعمـیم داده شود. هر گاه اجازه دهید که مقدار یک مکان تابع اختیاری از مقادیر مکان و از نزدیکتـرین همسـایه بـرروی مرحلـه زمـانی قبلـی انتخاب شود،در آن صورت یک گروه از قوانین بدست می آید:

$$ai(t+۱)=f(ai-۱(t), ai(t), ai+۱(t)) \qquad \text{(معادله ۲-۸)} \qquad [۱۱]$$

یک دستگاه علائم ساده در نمودار ۷ نشان داده شده است و برای ۲۵۶ قانون ازاین نوع،قانون عددی تعیین می شود. قانون عـددی معادله ۲-۱،در این دستگاه ،۹۰ می باشد.



شکل۲-۷: نحوه اعمال قانون ۹۰ در یک آتوماتای سلولی ساده

احکام کلی اضافی به هر مکان در آتوماتای سلولی این امکان را می دهد تا یک عدد اختیاری از مقادیر k را انتخاب کند.

به طوریکه:[۱۱]

$$a_i^{(t+1)}=f(a_{i-1}^{(t)}, \ldots, a_{i+r}^{(t)}) \qquad \text{(معادله ۹)}$$

تعداد قوانین مختلف با k داده شده و r به صورت k^{2r+1} گسترش می یابد و بنابراین حتـی بـرای k و r کوچک.تصـویر ۲-۸ نشان دهنده نمونه های تکاملی (طبق تعدادی از قوانین معمولی با مقادیر مختلف kوr می باشد. هر قانون منجر به نمونه هایی می شود که به طور جزئی با یکدیگر متفاوتند. اگر چه نمونه های مذکور نتیجه بسیار پیچیده چشمگری را نشان می دهد:بـه نظـر مـی رسد که همه نمونه ها تنها دارای چهار دسته وگروه کیفیتی هستند.این گروه های اساسی عملکرد از لحاظ تجربی به صـورت زیـر مشخص می شوند:

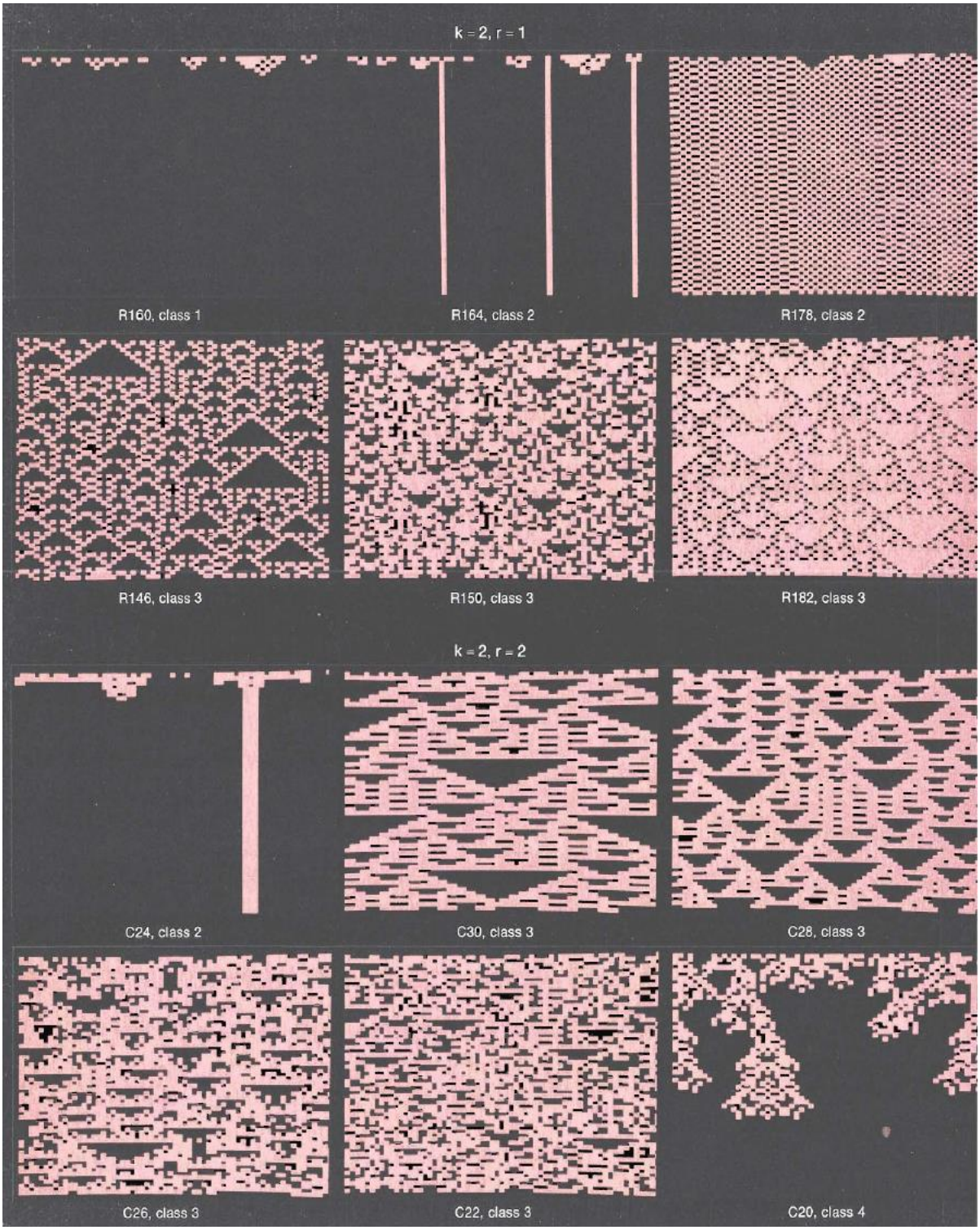
گروه اول- تکامل منجر به حالت متشابه می شود و در آن همه مکان ها دارای مقدار صفر هستند:

گروه دوم- تکامل منجر به یک مجموعه از ساختارهای ثابت یا ادواری می شود،به گونه ای که ساده و مجزا هستند.

گروه سوم- تکامل منجر به یک نمونه بی نظم می شود.

گروه چهارم- تکامل منجر به ساختارهای پیچیده و گاهی اوقات با دوام می شود.

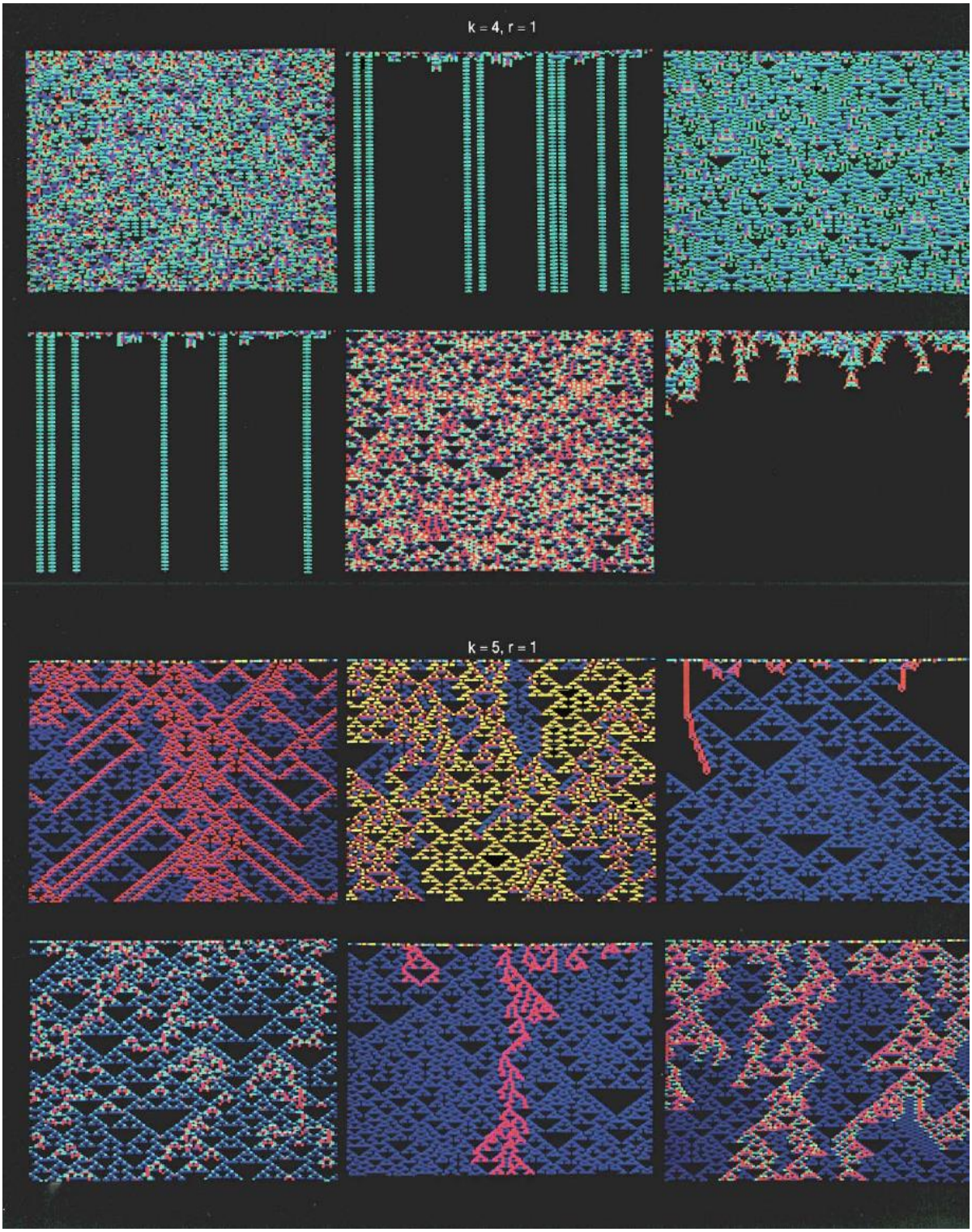
نمونه های این گروه ها در شکل ۲-۸نشان داده شده اند.



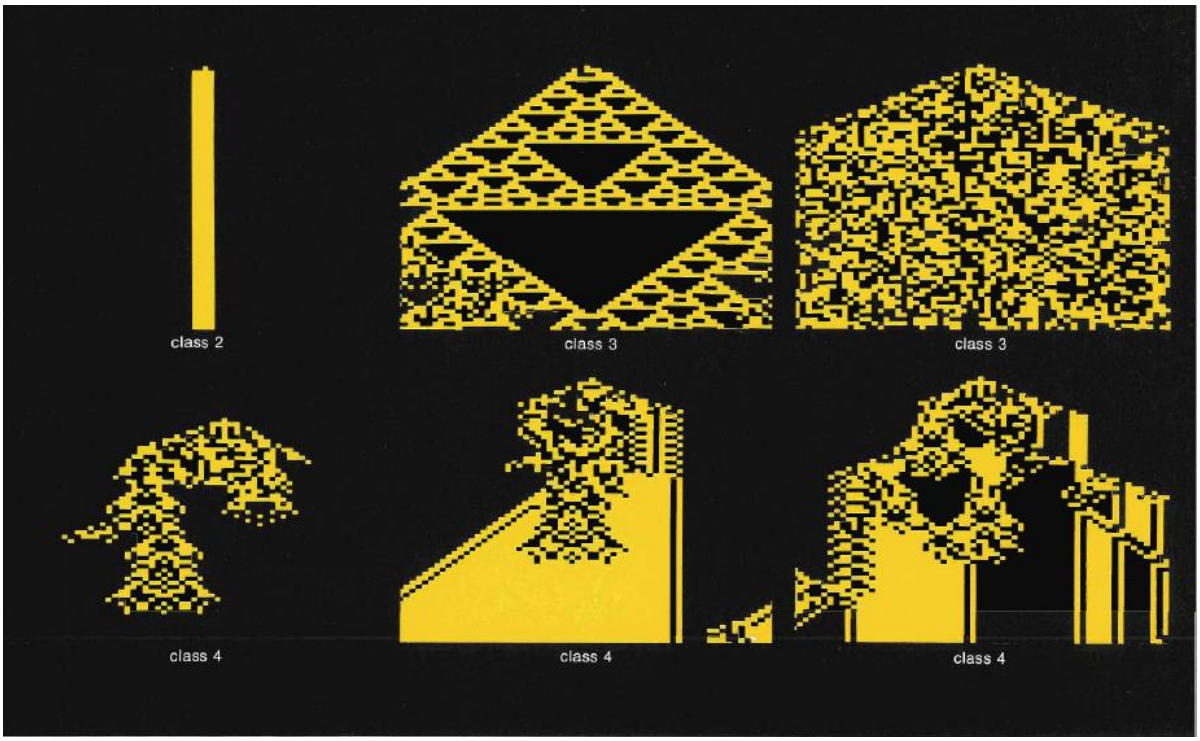
شکل ۲–۸: شکل حاصل از اعمال برخی قوانین در آتوماتای سلولی ساده و کلاس هر کدام


k = 3, r = 1
k = 3, r = 2

ادامه شکل



ادامه شکل ۲–۸



شکل۲-۹: نحوه گسترش هر یک از چهار کلاس آتوماتای سلولی ساده و تفاوت آنها

وجود چهار گروه یا دسته کیفیتی بیانگر جهان شمولی در عملکرد آتوماتای های سلولی می باشد:بسیاری از مشخصه های آتوماتای سلولی به گروهی بستگی دارند که در آن قرار می گیرند(نه به جزئیات دقیق تکامل آنها)چنین جهان شمولی با جهان شمولی در موازنه مکانیک آماری پدیده های اساسی قابل قیاس است (اگر چه احتمالا از لحاظ ریاضی نا مربوط می باشد). در این مورد،بسیاری از سیستم ها با طرح کاملا مختلف و مفصل در گروه هایی با توان های اساسی یافت می شوند و به طور کلی به مشخصه های هندسی سیستم ها وابسته اند .

۲-۵ عمومیت در آتوماتای سلولی

به منظور ادامه آنالیز جهان شمولی در آتوماتای سلولی می بایست ابتدا، تعاریف کمی تر گروه- های بالا را شناسایی کرد. یک روش به منظور چنین تعاریفی بررسی درجه پیش بینی پذیری نتیجه آتوماتای سلولی تکامل می باشد(بادادن معلومات و اطلاعات

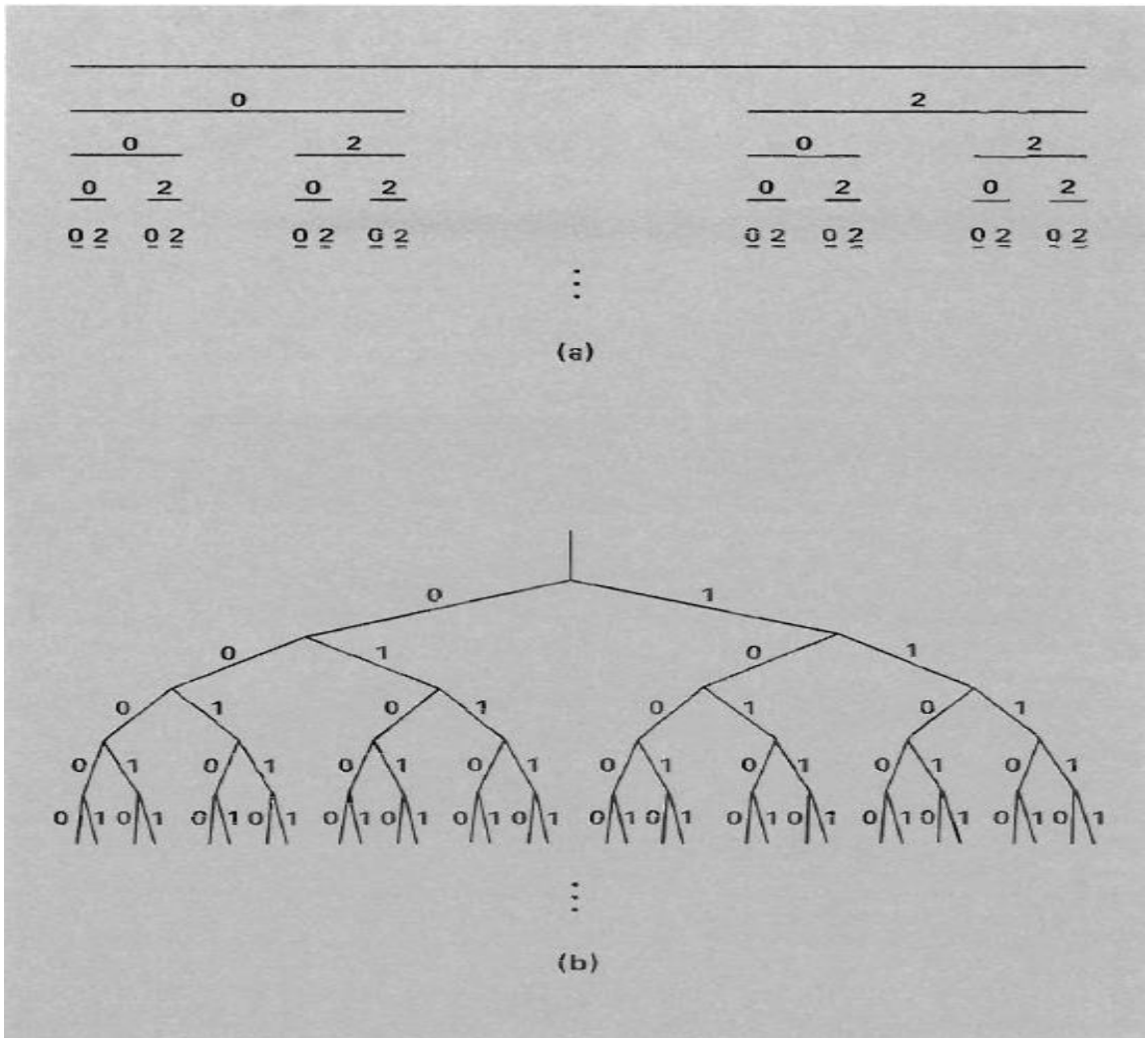
حالت اولیه). برای گروه اول آتوماتای سلولی و پیش بینی کامل آن،جزئی است. آتوماتای سلولی گروه دوم،دارای مشخصه ای است و تاثیرات مقادیر مکان ویژه در فاصله ای متناهی تکثیر می یابند. بنابراین یک تعیین در مقدار مکان اولیه منفرد تنها بر ناحیه متناهی مکان های اطراف آن تاثیر می گذاردحتی بعد ازتعداد نا محدودی مرحله زمانی)این عملکرد در شکل ۲-۹، نشان داده شده و بیانگر آن است که پیش بینی مقدار مکان نهایی مستلزم دانستن معلومات از مجموعه محدودی از مقادیر مکان اولیه می باشد. در مقابل تغییرات صورت گرفته در مقادیر مکان اولیه(در گروه ۳)و در آتوماتای سلولی(شکل۲-۹)با تقریبا در سرعتی محدود،تکثیر می شوند. بنابراین با گذر زمان برمکان های دورتر تاثیر می گذارند. مقدار یک مکان ویژه پس از بسیاری از مراحل زمانی به تعدادفزاینده مقادیر مکان اولیه بستگی دارد.اگر حالت اولیه نا منظم باشد،در آن صورت این وابستگی منجر به توالی نا منظم مقادیر می شود(برای یک مکان ویژه)در آتوماتای سلولی گروه سوم،پیش بینی مقدار یک مکان در زمان نامحدود مستلزم داشتن معلومات در زمینه تعداد نامحدودی از مقادیر مکان اولیه می باشد. آتوماتای سلولی گروه چهارم بوسیله درجه ای بیشتر از پیش بینی ناپذیری تشخیص داده می شوند.

ممکن است آتوماتای سلولی گروه دوم به عنوان فیلترهایی در نظر گرفته شوند که مشخصه های ویژه حالت اولیه را انتخاب می کنند. مثلا،آتوماتای سلولی گروه دو،در توالی اولیه ۱۱۱ زنده می مانند. اما دیگر مکان ها به غیر از این توالی به مقدارصفر می رسند. چنین آتوماتای سلولی برای پردازش تصویر دیجیتالی از اهمیت عملی برخوردارند:و ممکن برای انتخاب و افزایش نمونه های ویژه پیکسلی به کار روند. پس از یک دوره طولانی،هر آتوماتای سلولی از گروه ۲،به صورت یک حالتی تکمیل می شوند،هر حالت شامل قطعات و مکان های غیر صفری است که بوسیله یک سری نواحی در قسمتهای غیر صفر،تفکیک می شوند. قطعات دارای فرم ماده ای هستند و معمولا شامل تکررهای مقادیر مکانی ویژه یا توالی هایی از این مقادیر می باشند. قطعات مذکور با گذر زمان تغییر نمی کنند یا بین تعدادی حالات می چرخند.

در حالیکه آتوماتای سلولی گروه ۲،برای ارائه ساختارهای مقاوم با دوره های کوچک تکمیل می شوند اما آتوماتای سلولی گروه۳،عملکرد نا منظم را پریودیک را نشان می دهد. با وجود بی نظمی نمونه های تولید شده توسط آتوماتای سلولی گروه۳،کاملا تصادفی نیستند. در حقیقت همان طور که برای مثال معادله ممکن است عملکرد خود سازمان دهی را نشان دهند. علاوه بر این و مجددا در مقابل آتوماتای سلولی گروه ۲،ویژگی آماری حالتهای ایجاد شده توسط بسیاری از مراحل زمانی

آتوماتای سلولی گروه۳،تقریبا برای همه حالتهای اولیه احتمالی مشابه هستند. بنابراین عملکرد طولانی مدت آتوماتای سلولی گروه۳،بوسیله این ویژگی های آماری رایج تعیین می شوند.

ترکیبات آتوماتای سلولی نامحدود شامل یک توالی نا محدود از مقادیر مکانی می شوند. این مقادیر می توانند به عنوان ارقام در یک عدد حقیقی تلقی شوند:به طوریکه هر ترکیب کامل با یک عدد حقیقی منفرد،مطابقت می کند. اگر چه توپولوژی اعداد حقیقی برای ترکیبات همانند یک عدد طبیعی عمل نمی کند در عوض ترکیبات یک آتوماتای سلولی نا محدود مجموعه کانتور را تشکیل می دهند. نمودار۱۰،نشان دهنده دو طرح برای این مجموعه می باشد.



شکل ۲-۱۰: مراحل ایجاد ساختار کانتور که در a با استفاده از اعداد در مبنای ۱۰ و در b با استفاده از اعداد مبنای ۲ ایجاد شده است.

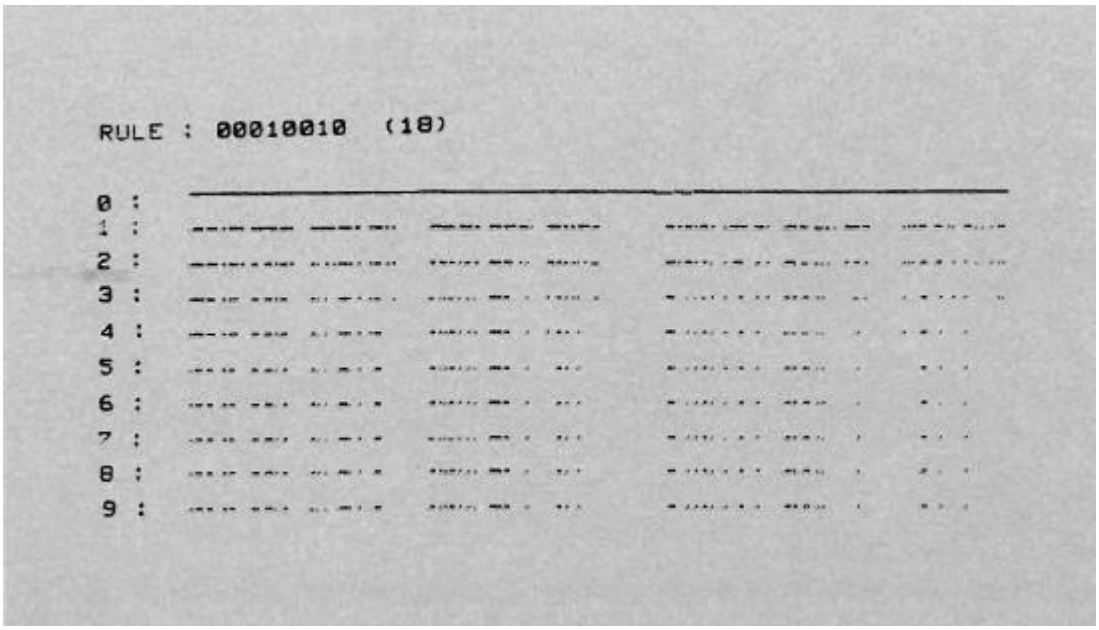
در طرح (a)نمودار۱۰،در فاصله۱-می توان با مجموعه اعداد حقیقی شروع کرد. در ابتدا ،نیمه فاصله را درنظرنمی گیرند،آنگاه،هر فاصله باقی می ماند. در حد گیری،مجموعه شامل تعداد نا محدودی نقطه منفصل می باشد. اگر موقعیتی در فاصله با پایانه ها نشان داده شوند،در آن صورت،برای حفظ نقاطی که موقعیتهایشان توسط پایانه های غیر یک نشان داده می شود،طرح مذکور دیده می شود یک مشخصه مهم از مجموعه محدود کننده همان خود متشابهی یا فرم کسری است یک قطعه از مجموعه در حین بزرگ شدن از کل آن قابل تشخیص نیست. از لحاظ ریاضی این خود متشابهی که برای حد نمونه دو بعدی شکل ۲-۳،یافت شد قابل قیاس می باشد.در طرح (b) از نمودار ۱۰ مجموعه کانتور از برگ های یک درخت دو گانه نامحدود تشکیل می شود. هر نقطه در مجموعه بوسیله یک مسیر منحصر به فرد در ریشه درخت بدست می آید. مسیر مذکور بوسیله یک توالی نامحدود از ارقام دو تایی تعیین می شود و در آن،ارقام متوالی نشان می دهند که آیا در هر سطح متوالی از درخت،شاخه سمت چپ بدست می آید یا سمت راست. هر نقطه در مجموعه کانتور به طور منحصر به فرد با یک توالی نامحدود از ارقام و نیز با یک ترکیب از آتوماتای سلولی نامحدود مطابقت می کند. تکامل آتوماتای سلولی نیز بانگاشتهای تکرار شده مجموعه کانتور و حتی خودش مطابقت می کند. این تفسیر از آتوماتای سلولی منجر به قیاس هایی با تئوری نگاشتهای تکرار شده از فواصل خط حقیقی می شود.

مجموعه های کانتور بوسیله ابعادشان پارامتری می شوند. یک تعریف ساده از بعد براساس طرح (a)نمودار ۱۰ به این صورت است. تقسیم کردن فاصله۱-۰ به knbins (هرعرض از k-n) آنگاه اجازه دهید تا $N(n)$ تعداد این بین ما باشد به گونه ای که نقاط مجموعه را در بر بگیرد. برای n بزرگ،این عدد طبق زیر عمل می کند: [۱۲]

$N(n)\sim k^{dn}$ (معادله ۲-۱۰)

و d به صورت بعد مجموعه ای از مجموعه کانتور تعریف می شود. اگر یک مجموعه شامل همه نقاط در فاصله ۱-۰ شود آنگاه با این تعریف،ابعاد آن به ساگی یک می شود. به طور مشابه،هر عدد متناهی از بخش های خط حقیقی،یک مجموعه را با بعد ۱،تشکیل می دهند. اگر چه،مجموعه کانتور در طرح (a) که شامل تعدادی نا محدود از قطعات منفصل می باشد. طبق معادله ۲، $\left(\log_3^2 = 0.03\right)$ دارای یک بعد است.

یک تعریف منتخب از بعد با تعریف قبلی برای اهداف کنونی سازگار است (طبق خود متشابهی).مجموعه کانتور از طرح(a) را نمودار ۱۰ بدست آورید. بوسیله بزرگنمایی ضریب k-m مجموعه را مختصر کنید. به واسطه خود متشابهی،کل مجموعه مشابه عدد$M(m)$ می شود(برگرفته از کپی های این کپی های مختصر شده). برای m بزرگتر $m(m)\sim kdn$ ،در اینجا مجددا d به صورت بعد مجموعه تعریف می شود.



شکل ۲-۱۱: شکل حاصل از اعمال قانون ۱۰ برای هر یک از ۱۰۲۴ حالت در آتوماتای سلولی ساده

با این تعاریف،بعد مجموعه کانتور درهمه ترکیبات احتمالی برای یک آتوماتای سلولی تک بعدی،یک می شود. یک مجموعه کلی نا منظم که در آن هرترکیب احتنالی با احتمال برابر رخ می دهد، دارای بعد یک است. نمودار ۱۱،نشان دهنده عملکرد احتمالات برای ترکیبات از یک آتوماتای سلولی معمولی است و به عنوان تابعی از زمان در نظر گرفته شده که از یک چنین مجموعه اولیه نا منظم آغاز می شود. همان طور که از برگشت ناپذیری تکامل آتوماتای سلولی انتظارمی رود بوسیله گراف انتقال حالت(شکل۲-۶)،نشان داده می شود،ترکیبات مختلف از احتمالات مختلف بدست می آیند(با ادامه یافتن تکامل) و احتمالات این ترکیبات به صفر کاهش می یابد.این پدیده،درکاهش دادن ترکیبات مراحل زمانی متوالی،(نمودار ۱۱)مشهودات مجموعه ای از ترکیب که پس از مراحل زمانی زیاد در تکامل آتوماتای سلولی به صورت احتمالات غیر صفر باقی می مانند،متشکل از جذب

کننده ها می باشند(برای تکامل)مجددا این مجموعه یک مجموعه کانتور است:برای مثال در نمودار ۱۱،بعد آن $\log_2 k=0$ است.در اینجا$k=1,755$ ،که یک پاسخ حقیقی از معادله چند جمله ای (پلی نامیال) $Z^3-Z^2+2X-1=0$ می باشد.هر چه برگشت ناپذیری در تکامل آتوماتای سلولی بیشتر باشد،بعد مجموعه کانتور کوچکتر می شود و این میزان با جذب کننده های تکامل مطابقت می کند. اگر مجموعه جذب کننده ها برای یک آتوماتای سلولی دارای بعد یک باشد،در آن صورت،همه ترکیبات آتوماتای سلولی در زمان های طولانی رخ می دهند. اگر مجموعه جذب کننده ها دارای بعدی کمتر از یک باشد،در آن صورت کسر کوچکی از همه ترکیبات احتمالی پس از مراحل زمانی تکامل زیاد ایجاد می شوند. مجموعه های جذب کننده برای بیشتر آتوماتای سلولی گروه ۳،دارای ابعاد کمتر از ۱ می باشد. برای آن دسته از آتوماتای سلولی گروه۳،که نمونه های منظمی را ارائه می دهند،هر چه نمونه منظم تر باشد بعد مجموعه جذب کننده کوچکتر می شود،این آتوماتای سلولی برگشت ناپذیرند و بنابراین دارای درجه بالاتری از خود–سازمان دهی هستند. [۱۲]

بعد یک مجموعه از ترکیبات آتوماتای سلولی،مستقیما متناسب با آنتروپی محدود شونده می باشد(در هر مکان از توالی مقادیر مکانی که تشکیل دهنده ترکیبات هستند)اگر بعد مجموعه یک بود به گونه ای که توالی های احتمالی مقادیر مکانی رخ می داد،در آن صورت،آنتروپی این توالی ها ماکسیمم می شد. ابعاد کمتر از یک با مجموعه هایی مطابقت دارند که در آنها بعضی از توالی های مقادیر مکانی غایب باشد،بدین طریق آنتروپی کاهش می یابد. بنابراین بعد جذب کننده برای یک آتوماتای سلول مستقیما مرتبط با آنتروپی محدود کننده می باشد و از مجموعه کلی نا منظم حالتهای اولیه آغاز می شود.

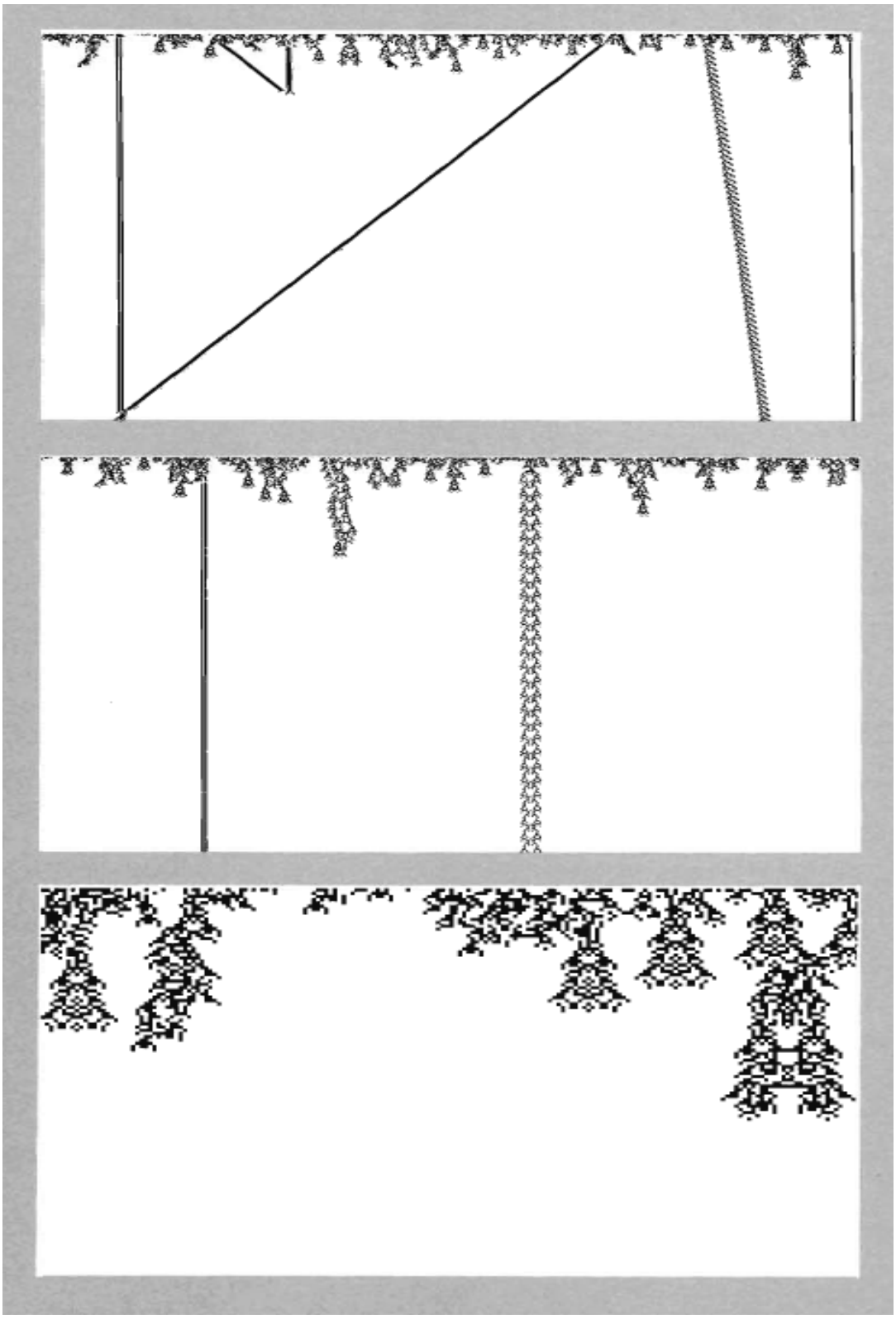
بعد،تنها یک ساختار از مجموعه ترکیبات رادر اندازه بسیار درشت ارائه می دهد که در طولانی مدت و در یک آتوماتای سلولی بدست می آید. ممکن است تئوری رسمی زبان،مشخصه کامل تری از مجموعه را ارائه دهد. زبان شامل مجموعه ای از لغات هستند که در شماره و ارقام نا محدودند،و از یک توالی حروف(طبق قوانین دستوری ویژه)تشکیل می شوند. ترکیبات آتوماتای سلولی از لحاظ زبان رسمی،قابل قیاس و مشابه لغات هستند. در زبان مذکور،حروف،همان مقادیر احتمالی k،در مکان از آتوماتای سلولی می باشند. سپس یک گرامر یا دستورزبان مشخصه ای موجزا را برای یک مجموعه از ترکیبات آتوماتای سلولی ارائه می دهد.

زبان ما ممکن است طبق پیچیدگی ماشین ها یا رایانه ها طبقه بندی شوندو برای آنها ضروری هستند. یک گروه ساده از زبان ها بوسیله گرامر های (دستورزبان های با قاعده تعیین می شوند و ممکن است از طریق ماشین های متناهی حالت ایجاد شوند. ماشین متناهی حالت بوسیله گراف انتقال حالت،نشان داده می شود. واژه ها یا لغات احتمالی در یک گرامر بوسیله عبور کردن از همه مسیرهای احتمالی در یک گراف انتقالی حالت بدست می آیند. ممکن است این واژه ها از طریق عبارات با قاعده تعیین شده و شامل توالی های طول متناهی و موارد تکرار شده اختیاری می باشند. مثلا عبارت منظم و با قاعده ۱*(۰۰)۱ نشان دهنده همه توالی هاست حتی توالی های متشکل از عدد صفر و در کنار یک جفت (۱)قرار می گیرد. مجموعه ای از ترکیبات بدست آمده در زمان های طولانی(در آتوماتای سلولی گروه۲)برای تشکیل یک زبان با قاعده بدست آمده اند. احتمالا جذب کننده های گروه های دیگر آتوماتای سلولی با زبان های پیچیده تر مطابقت دارند.

۲-۶ مقایسه با تئوری سیستم های دینامیکی

عملکرد سه گروه آتوماتای سلولی تا کنون توضیح داده شده این عملکرد ها با عملکرد سه گروهی که در راه حل های معادلات دیفرانسیلی یافت شدند،مشابه و قابل قیاس است. برای بعضی از معادلات دیفرانسیلی،جوابها (راه حل ها)با شرایط اولیه بدست می آیند و به نقطه ثابتی در زمان های طولانی نزدیک می شوند.این عملکرد با عملکرد آتوماتای سلولی گروه۱،قابل قیاس است. در گروه دوم معادلات دیفرانسیلی،راه حل محدود کننده(حدی)در زمان های طولانی،سیکلی است که در آن پارامترها به طور ادواری با زمان تغییر می کنند. این معادلات با آتوماتای گروه دوم،قابل قیاس هستند. در نهایت،بعضی از معادلات دیفرانسیلی برای نشان دادن عملکرد نا منظم و پیچیده یافت می شوند که البته این مورد به شرایط اولیه آنها بستگی دارد. از طریق شرایطاولیه ای که توسط کسرهای اعشاری تعیین می شوند راه حل و جواب این معادلات دیفرانسیلی به درجه بالاتر ارقام بستگی پیدا می کند. این پدیده به رابطه مقدار مکان ویژه با مقادیر اولیه دورتر در تکامل آتوماتای سلولی گروه ۳،شباهت دارد. جوابهای این گروه نهایی از معادلات دیفرانسیلی به صورت جذب کننده های نا معمول یا نا منظم متمایل می شوند. و در مقایسه مستقیم با آنهایی که در آتوماتای سلولی گروه سوم یافت شدند. مجموعه های کانتور را تشکیل می دهند. تطابق بین عملکرد گروه ها در آتوماتای سلولی مشخص شده، نمونه هایی که در سیستم های دینامیکی مستمر یافت شدند کلیت و عمومیت این گروه ها را تایید می کنند. علاوه

بر این،سادگی بیشتر ریاضی در آتوماتای سلولی نشان می دهد که بررسی عملکردآنها ممکن است عملکرد سیستم هـای دینـامیکی مستمر را توضیح دهد.



شکل ۲-۱۲: شکل حاصل از توسعه کلاس ۴ آتوماتای سلولی با مقادیر اولیه متفاوت

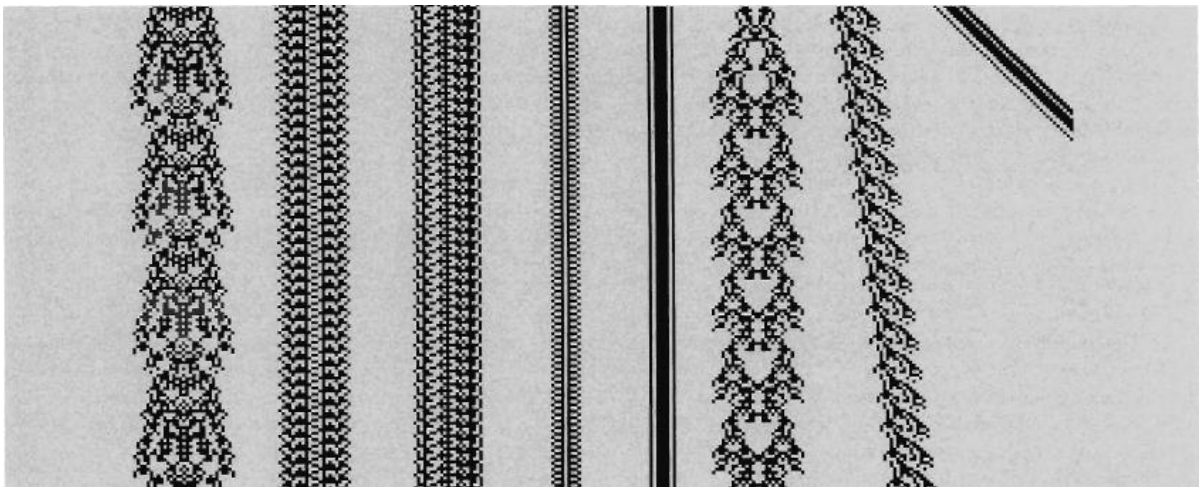
۲-۷ یک کلاس محاسبه ای عمومی از آتوماتای سلولی

شکل ۲-۱۲،نشان دهنده نمونه هایی هستند که بوسیله تکامل حالتهای اولیه نا منظم بدست آمده اند(طبق قانون آتوماتای سلولی گروه ۴)در بیشتر موارد،همه مکان ها در نهایت از بین می روند. اگر چه در بعضی موارد ساختارهای مقاومی که برای یک زمان نا محدود باقی می مانند،بوجود می آیند،وتعدادی از این ساختارها با زمان تکثیر می شوند. شکل ۲-۱۳،نشان دهنده همه ساختارهای مقاومی است که از حالات اولیه با مکان های غیر صفر بوجود می آیند(در ناحیه ای با ۲۰ مکان یا کمتر) بر خلاف ساختارهای ادواری آتوماتای سلولی گروه ۲،این ساختارهای مقاوم،دارای نمونه های ساده نیستند. علاوه بر این،ساختارهای تکثیری این امکان را فراهم می کنند که مقادیر مکانی در یک موقعیت بر مکان ها را دور تاثیر بگذارند(پس از یک زمان طولانی)هنوز هم در یک سیستم دینامیکی مستمر،هیچ عملکرد مشابهی ،مشاهده نشده است.

پیچیدگی مشخص در عملکرد آتوماتای سلولی گروه ها،نشان دهنده این فرضیه است که سیستم های مذکور ممکن است بتوانند یک محاسبه کلی را انجام دهند. یک کامپیوتر می تواند به عنوان سیستمی در نظر گرفته شود که در آن قوانین محدود برای تبدیل توالی اولیه(۰ و۱)به توالی نهایی (۰ و۱) به کار می روند. توالی اولیه را می توان به عنوان برنامه ای در نظر گرفت که طبق آن داده ها در حافظه کامپیوتر ذخیره می شوند. آتوماتای سلولی را به عنوان رایانه ها در نظر می گیرند. ترکیبات اولیه آنها نشان دهنده برنامه ها و داده های اولیه می باشد،و ترکیبات آنها پس از یک زمان طولانی شامل نتایج محاسبات می شوند.

یک سیستم زمانی یک رایانه (کامپیوتر)کلی محسوب می شود(با ارائه یک برنامه اولیه مناسب)که تکامل زمانی آن بتواند هر الگوریتم محدود را اجرا کنند.بنابراین یک کامپیوتر عمومی تنها باید برنامه نویسی مجدد شود نه اینکه از نوساخته شود بدین طریق،هر محاسبه احتمالی را اجرا می کند. اگر آتوماتای سلولی یک کامپیوتر عمومی باشد(با یک قانون ثابت برای تکامل زمانی آن)در آن صورت ترکیبات اولیه مختلف را باید برای همه برنامه های احتمالی،کد گذاری کرده تنها روش شناخته شده برای اثبات اینکه یک سیستم ممکن است به صورت یک کامپیوتر عمومی عمل کند این است که نشان دهیم توانایی ها و امکانات محاسبه ای (تخمینی)آن معادله سیستم دیگری است که هم اکنون به عنوان یک کامپیوتر عمومی در نظر گرفته می شود. رساله church-Turing بیان می کند که ممکن است قابلیتهای محاسبه ای هیچ سیستمی بیشتر از کامپیوترهای عمومی نباشد.رساله مذکور بوسیله تعادل مدل های محاسبه ای مانند ماشین های Turingسیستم های کنترل و دستکاری رشته ای شبکه های ایده آل عصبی

کامپیوترهای دیجیتالی،و آتوماتای سلولی حمایت می شود. در حالیکه سیستم های ریاضی بات نیروی محاسبه ای فراتر از کامپیوترهای همگانی) مد نظر هستند،اما به نظر می رسد که چنین سیستمی با قطعات فیزیکی نتواند ساخته شود.این فرضیه در اصل می تواند با نشان دادن این که همه سیستم های فیزیکی از طریق یک کامپیوتر عمومی شبیه سازی می شوند تایید شود.



شکل۲-۱۳: پایداری اشکال تولید شده با استفاده از کلاس ۴ آتوماتای سلولی

یک آتوماتای سلولی می تواند تایید شود که دارای قابلیت محاسبه عمومی است(بوسیله شناسایی ساختارهایی که همانند قطعات ضروری کامپیوترهای دیجیتالی عمل می کنند همانند سیستم ها،دروازه های NAND،حافظه ها و ساعتها،ساختارهای مقاوم نشان داده شده در شکل ۲-۱۳،بسیاری از قطعات لازم را فراهم می کنند و این نشان می دهد که آتوماتای سلولی تصاویر ۲-۱۳ و۲-۱۲،یک کامپیوتر عمومی می باشد. یک قطعه مهم و فراموش شده،ساعتی است که توالی نا محدود از پالس ها را ایجاد می کند. از یک ترکیب اولیه که شامل تعداد محدودی مکان غیر صفر است آغاز می شود. چنین ساختاری وجود داشته باشد بدون شک می توان آن را با بررسی دقیق مشخص کرد،اگر چه احتمال زیادی وجود دارد که بتوان آن را با هر تحقیق جامع و علمی مشخص کرد. اگر آتوماتای سلولی شکل های ۲-۱۳ و۲-۱۲ توانایی محاسبه عمومی را داشته باشد. در آن صورت بر خلاف طرح بسیار ساده آن می تواند به طور اختیاری عملکرد پیچیده ای داشته باشد.

تایید شده که چندین آتوماتای سلولی پیچیده توانایی محاسبه عمومی را دارند. یک آتوماتای سلولی یک- بعدی با ۱۸ مقادیر احتمالی در هر مکان مطابق و معادل با ساده ترین ماشین عمومی Turing می باشد. در دو بعد،چندین آتوماتای سلولی با دو حالت در هر مکان و تقابلات بین نزدیکترین مکان مجاور معادل و مطابق با کامپیوترهای دیجیتالی عمومی می باشند. معروف

ترین آتوماتای سلولی همان Game of life است که در اوایل دهه ۷۰ توسط کونوای اختراع شد و تا بـه حـال نیزشـبیه سـازی شده است. ساختارهای مشابه با ساختارهای شکل ۲-۱۳،در بازی زندگی (Game of life) شناسایی شده انـد. عـلاوه بـر ایـن پس از کاوش زیاد،یک ساختار ساعتی(دوبله شده به نام اسلحه گلایدر)یافت شد. [۱۳]

طبق تعریف،هرکامپیوتر عمومی در اصل به وسیله کامپیوتر دیگری از این نوع شبیه سـازی مـی شـود. ایـن شـبیه سـازی،با تقلیـد عملیات مقدماتی در کامپیوتر عمومی اول و توسط یک سری عملیات در کامپیوتر عمومی دوم ادامه می یابد(همان گونه که در یک برنامه تفسیر کننده دیده می شود)به طور کلی شبیه سازی بوسیله یک فـاکتور ثابـت و محـدود سـریع تـر یـا آهسـته تـر رخ مـی دهد(مستقل و جدای از اندازه یا مدت محاسبه) بنابراین عملکرد یک کامپیوترعمومی،ورودی خاصی را ارائـه مـی دهـد و ممکـن است تنها در زمانی از درجه مشابه تعیین شود،برای به راه انداختن کامپیوتر عمومی به این زمان نیاز اسـت. بـه طـورکلی عملکـرد یک کامپیوتر جامع و عمومی را نمی توان پیش بینی کرد و تنها بوسیله یک روش و فرآیند مرتبط با مشاهده خـود کـامپیوتر جـامع آن را تعیین می کنند.

اگر آتوماتای سلولی گروه ۴ واقعا کامپیوترهای جامع باشند در آن صورت عملکرد آنها را به طور کامل غیر قابل پیش بینی در نظـر می گیرند. برای آتوماتای سلولی گروه۳،مقادیرمکان های ویژه (پس از یک زمان طولانی)به تعداد فزاینده ای از مکـان هـای اولیـه بستگی دارند. برای آتوماتای سلولی گروه ۴،این وابستگی،یک الگوریتم از پیچیدگی اختیاری می باشد و مقادیر مکان ها می توانند ضرورتا توسط مشاهده عینی تکامل آتوماتای سلولی مشخص شود. پیش بینی ناپذیری آتوماتـای سـلولی گـروه ها،نشـان دهنـده سطح جدیدی از عدم قطعیت عملکرد سیستم های طبیعی می باشد.

پیش بینی ناپذیری عملکرد کامپیوتر جامع نشان می دهد که قضیه های مرتبط با عملکرد محـدود کامپیوترهـای جـامع در دفعـات نامحدود نا مشخص هستند. مثلا مشخص نیست که آیا یک کامپیوتر جامع (با داده های ویژه)پس از یک زمان محـدود بـه حالـت ویژه ای از توقف خواهد رسید یا اینکه برای همیشه قدرت محاسبه ای خود را خواهد داشت. شبیه سازی های عینـی مـی تواننـد تنها برای مدتی محدود فعالیت داشته باشند. و بنابراین نمی توانند چنین عملکرد نا محدود زمانی را تعیین کنند. ایـن نتـایج بـرای بعضی از داده های سلولی گروه ها،کامپیوترهای جامع باشند. در آن صورت مشخص نیست که آیا یک حالت اولیـه ویـژه ترکیـب صفر را ایجاد می کنند یا نه یا اینکـه آیـا سـاختارهای مقـاوم را ایجـاد مـی کننـد. همـان گونـه کـه بـرای چنـین قضـیه هـای نـا

مشخص،طبیعی است،موارد ویژه می توانند قطعی می شوند. در حقیقت توقف آتوماتای سلولی شکل های ۲-۱۳ و۲-۱۲ برای همه حالتهای اولیه با مکان های غیر صفر(در ناحیه ای با ۲۰ مکان) توسط شبیه سازی عینی تعیین می شود. به طور کلی احتمال توقف یا کسری از ترکیبات اولیه ،ترکیب صفر را ایجاد می کنند و این رقم غیر قابل محاسبه است. اگر چه نتایج عینی برای نمونه های کوچک اولیه نشان می دهند که برای آتوماتای سلولی شکل های ۲-۱۳ و ۲-۱۲ این احتمال توقف حدود ۹۳٪ می باشد.

در یک ترکیب نا منظم و نا متناهی، همه توالی های احتمالی از مقادیر مکانی در چندین نقطه ظاهر می شوند. اگر چه احتمال آن بسیار کم است. هر کدام از این توالی ها،نشان دهنده یک برنامه احتمالی هستند؛بنابراین با حالت اولیه نا منظم نا محدود آتوماتای گروه ۴،می توان همه برنامه های احتمالی را اجرا کند. برنامه هایی که ساختارهای اختیاری و پیچیده را تولید می کنند،حداقل دارای احتمالات بسیار کم می باشند. مثلا در جایی روی خط نا متناهی که تکمیل کننده ساختار خود تکثیری است یک توالی باید رخ دهد. پس از یک دوره طولانی،این ترکیب به طور مکرر رخ می دهد و در نهایت بر عملکرد آتوماتای سلولی مسلط می شود. با وجودیکه احتمال برای وقوع یک ساختار خود تکثیری کم است(در حالت اولیه)اما احتمال عقبی و دورتر پس از مراحل زیاد زمانی از تکامل آتوماتای سلولی بسیار زیاد خواهد بود. احتمال آنکه عملکرد پیچیده تصادفی توسط مشخصه های حالت اولیه پدید آید. در آتوماتای سلولی گروه ۴ با حالت اولیه نا منظم و نا معین میکروکوزمی از هستی تلقی می شود.

در نمونه های جامع قوانین آتوماتای سلولی مشخش شده که با افزایش r وk عملکرد گروه۳،چشمگیر خواهد شد. عملکرد گروه ۴ تنها برای $r>1$ یا $k>2$ رخ میدهد؛و برای r و k بزرگتر رایج تر است اما درصد کمی خواهد داشت این حقیقت که آتوماتای سلولی گروه ۴ با سه مقدار از هر مکان و در نزدیکترین تقابل وجود دارند،نشان می دهد که آغاز پیچیدگی ساختار ضروری بوده و عملکرد پیچیده تصادفی را به شدت کاهش می دهد. اگر چه،حتی در میان سیستم هایی از طرح پیچیده تر تنها کسر کوچکی می تواند عملکرد پیچیده و تصادفی داشته باشد. و این نشان می دهد که بعضی از سیستم های فیزیکی می توانند بوسیله عملکرد گروه ۴ و محاسبه جامع مشخص شوند؛تکامل چنین سیستم هایی است که عامل ایجاد ساختارهای بسیار پیچیده می شود(یافت شده در طبیعت).

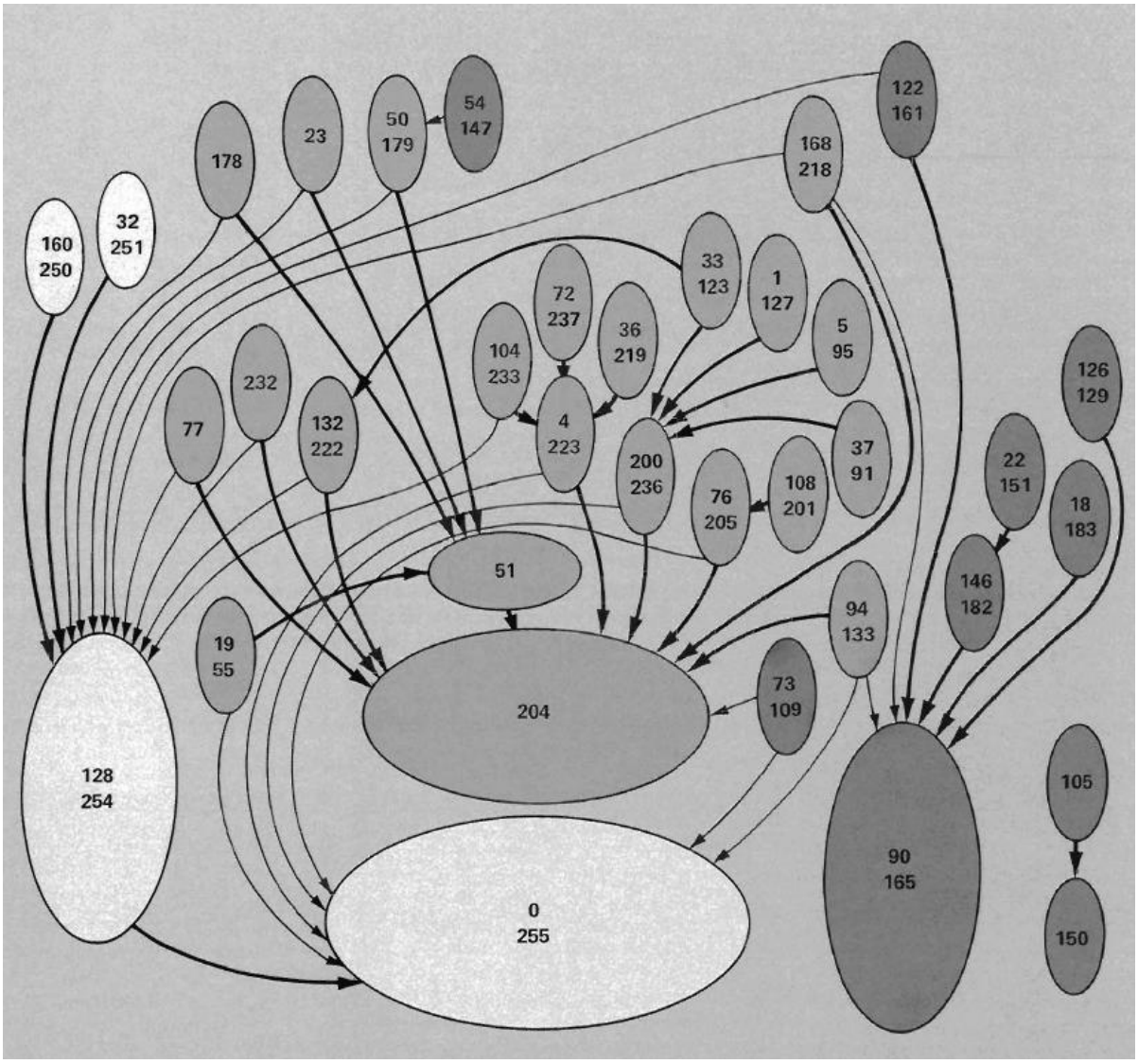
احتمال محاسبه جامع در آتوماتای سلولی نشان می دهد که در اصل محاسبات تصادفی ممکن است بوسیله آتوماتای سلولی صورت بگیرند. بر این اساس آتوماتای سلولی می توانند به عنوان کامپیوترهای عملی شبه پردازش کننده به کار روند. مکانیسم

های این پردازش اطلاعات در بیشتر سیستم های طبیعی پیدا شده اند و به نظر می رسد که بیشتر مشابه آتوماتای سلولی باشند تا ماشین های Turing یا کامپیوترهای دیجیتالی پردازش کننده سریال. بنابراین می توان فرض کرد که بسیاری از سیستم های طبیعی بوسیله آتوماتای سلولی بهتر شبیه سازی می شوند(نسبت به کامپیوترهای مرسوم و متداول)در اصطلاحات عملی شباهت آتوماتای سلولی منجر به مدارهای ادغام شده می شود یک آتوماتای جامع تک بعدی ساده،با یک میلیون مکان ویک مرحله زمانی به کوتاهی یک میلیاردم ثانیه،توسط تکنولوژی اخیر(ویفرسیکییون مجزا)ساخته شده است.البته اسلوب شناسی برنامه نویسی متداول برای چنین کاربرد کمی دارد. ارائه یک اسلوب شناسی جدید،مشکل است. اما مسئله و مبحث مهمی محسوب می شود. احتمالا اقداماتی نظیر پردازش تصویر که مستقیما مناسب آتوماتای سلولی است،در ابتدا مورد بررسی قرار گیرد. [۱۳]

۲-۸ پایه و اساس برای عمومیت

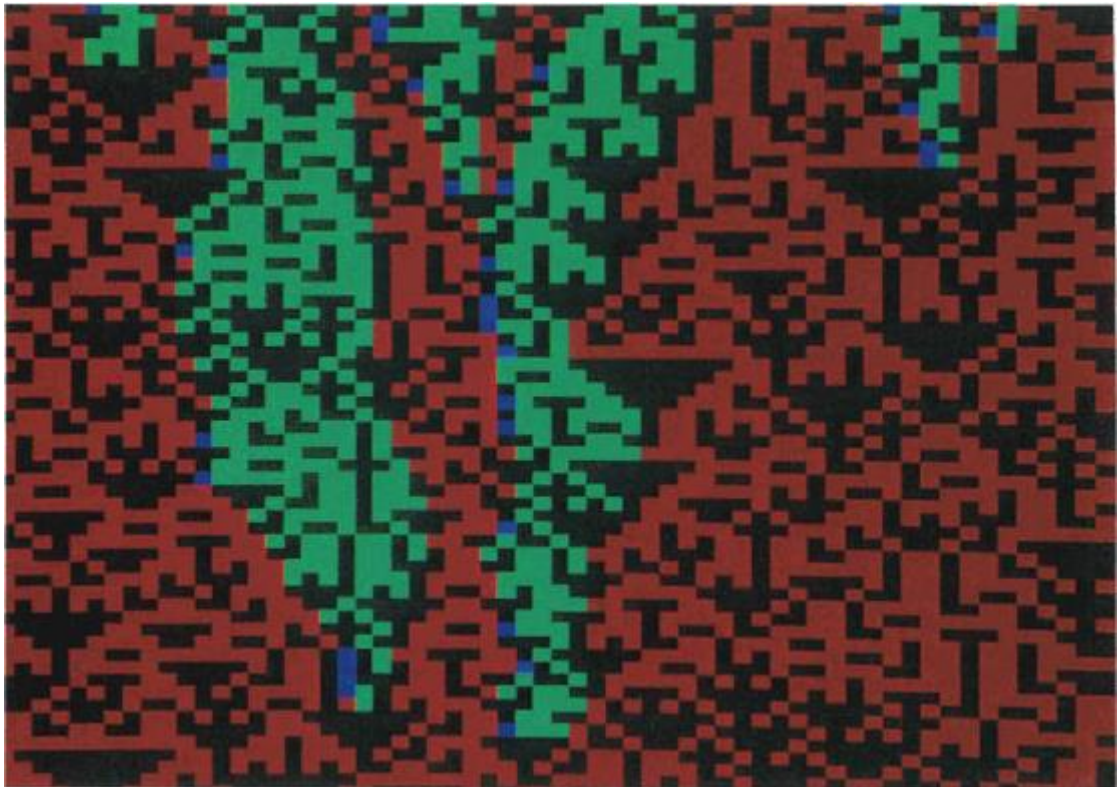
وجود چهار گروه از آتوماتای سلولی در بالا به عنوان نتیجه تجربی ارائه شده است .تکنیکهای تئوری محاسبه ای،معیار و دلیل را برای این نتیجه ارائه می دهند.

اولین مشاهده قاطع آن است که با حالتهای اولیه ویژه،یک آتوماتای سلولی می تواند همچون دیگر رفتار کند. در این روش،یک آتوماتای سلولی را مشابه و شبیه نمونه دیگر در نظر می گیرند.یک مکان مجزا و منفرد با یک مقدار ویژه در آتوماتای سلولی بوسیله،قطعه ای ثابت از مکان ها در دیگری شبیه سازی می شود. پس از تعداد ثابتی مرحله زمانی تکامل این قطعات،به تقلید تکامل مرحله زمانی مکان ها در آتوماتای سلولی اول می پردازد. مثلا مکان هایی با مقدار صفر و یک در آتوماتای سلولی اول می توانند بوسیله قطعات مکانی ۰۰ و ۱۱ (به ترتیب)در آتوماتای سلولی دوم شبیه سازی شوند،دو مرحله زمانی تکامل در آتوماتای سلولی دوم،با یک مرحله زمانی در آتوماتای اول مطابقت می کند. سپس با یک حالت اولیه ویژه که شامل ۱۱ و۰۰ (نه قطعات ۱۰ و۰۱)ممکن است آتوماتای سلولی دوم،آتوماتای اول را شبیه سازی کند.



شکل۲-۱۴: شبیه سازی شبکه ای برای قوانین آتوماتای سلولی ساده با k=۲ و r=۱

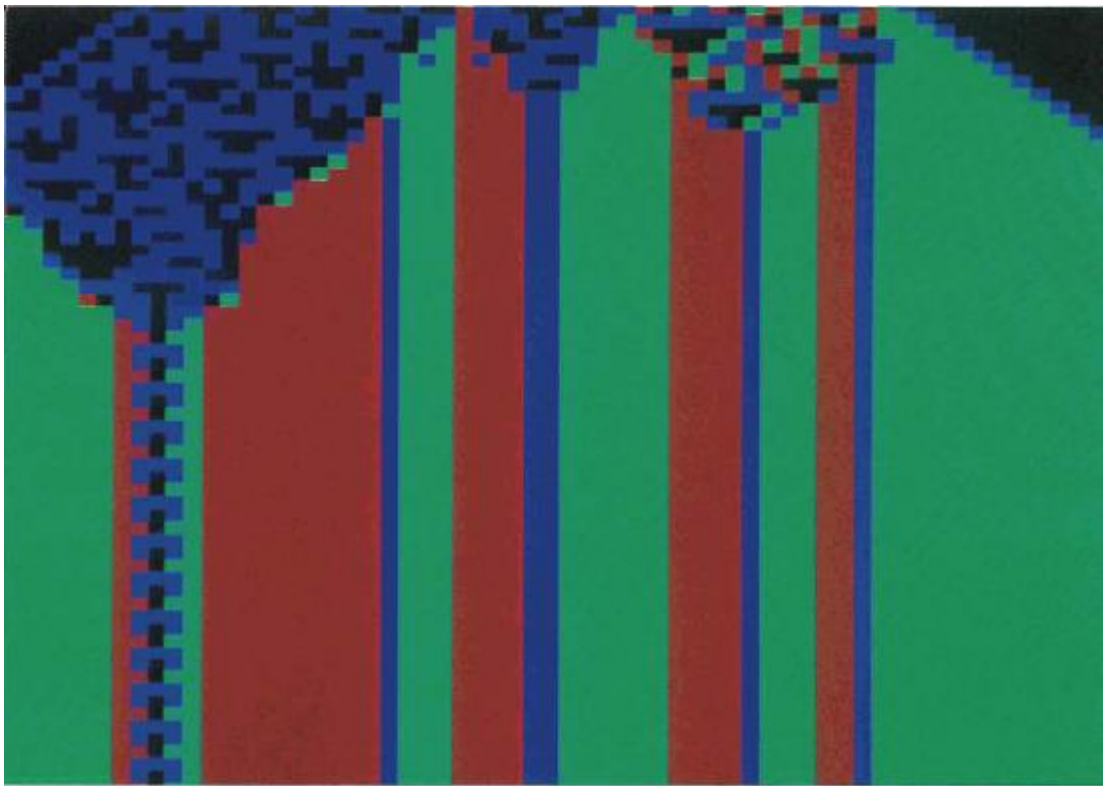
تصویر ۲-۱۴،شبکه ای را ارائه می دهد که نشان دهنده توانایی شبیه سازی آتوماتای سلولی متقارن با k=۲ و k=۱ است. اگر یک آتوماتای سلولی از لحاظ محاسبه ای جامع و کلی باشد،در آن صورت با کد گذاری طولانی می تواند هرآتوماتای سلولی دیگر را نیز شبیه سازی کند. بدین طریق می بایست مسیری از گره وجود داشته باشد با قانون خود را در گروه دیگر نشان دهد.



شکل ۲-۱۵: شکل حاصل از گسترش کلاس ۳ آتوماتای سلولی با اعمال قانون ۱۸ و مقدار اولیه تصادفی

نمونه ای از شبیه سازی یک آتوماتای سلولی بوسیله آتوماتای دیگر،همان شبیه سازی قانون جمع پذیری ۹۰ توسط قانون ۱۸ گروه سوم می باشد. آتوماتای سلولی قانون ۱۸ دقیقا مشابه آتوماتای سلولی قانون ۱۹ عمل می کند البته در صورتی که مکان های متناوب در ترکیب اولیه دارای مقدار صفر بوده ونیز مراحل زمانی متناوب مورد بررسی قرار گیرند. شکل ۲-۱۵،نشان دهنده تکاملی است که با قانون ۱۸ از یک حالت اولیه نا منظم مطابقت می کند. دوفاز به وضوح،مشخص هستند:فازی که در آن،مکان ها در موقعیتهایی با عدد گذاری مساوی دارای مقدار صفر هستند و فازی که در آن مکان ها در موقعیتهایی با عدد گذاری فرد دارای مقدار صفری باشند. حدهای بین این نواحی،مسیرهای تصادفی را طی می کنند و در نهایت به صورت جفت دار از بین می روند،بدین طریق سیستمی برجای می ماند که شامل قطعات و بخش های مکانی است که طبق قانون جمع پذیری ۹۰،تکمیل می شوند.

بنابراین شبیه سازی قانون ۹۰ توسط قانون ۱۸،ممکن است یک نمونه جاذب تلقی شود:از همه حالتهای اولیه آغاز می شود قانون ۱۸ نسبت به حالاتی که در آن قانون ۹۰،شبیه سازی می شود. به تکامل می رسد. به طور کلی انتظار می رود که بعضی از مسیرهای در شبکه شکل ۲-۱۴،جاذب باشند،در حالیکه بقیه مسیرها دافع هستند.



شکل ۲-۱۶: شکل حاصل از گسترش کلاس ۲ آتوماتای سلولی با اعمال قانون ۹۴

نتایج شبیه سازی مسیرهای دافع در شکل ۲-۱۶ نشان داده شده است: با حالتهای اولیه ویژه قانون ۹۴ قانون ۹۰ عمل می کند،اما هرگونه ناخالصی در حالتهای اولیه گسترش یافته و در نهایت بر تکامل سیستم غالب می شود.

آتوماتای سلولی گروه۱،دارای یک مسیر شبیه سازی جاذب در قانون صفر هستند. آتوماتای سلولی گروه ۲ دارای مسیرهای شبیه سازی جاذب در قانون ۲۰۴ هستند. یک فرضیه برای چنین مدارک و شواهدی بیان می کند که همه قوانین گروه۳،نشان دهنده شبیه سازی های جاذب بوده و قوانین جمع پذیر ۹۰ یا ۱۵۰ می باشد. شبیه سازی بوسیله مسدود کردن مقادیر مکانی مشابه با یک بلوک چرخشی یا عادی سازی مجدد گروه می باشد:قوانین جمع پذیر دارای ویژگی خاصی است به گونه ای که تحت چنین تغییر

و تبادلاتی ثابت می مانند. همان طور که اشاره شد آتوماتای سلولی گروه ۴ بوسیله وجود مسیرهای شبیه سازی شده قابل تشخیص اند و منجر به قانون آتوماتای سلولی دیگر می شود.به نظر می رسد هیچ مسیر ویژه ای به عنوان جاذب قابل تشخیص نباشد.

آتوماتای سلولی گروه های مختلف بوسیله عملکرد محدود کننده شان (تحت تغییر و تبادلات شبیه سازی)قابل تشخیص هستند. این روش نشان می دهد که طبقه بندی عملکرد کیفی آتوماتای سلولی می توانند به عوامل تعیین کننده سیستم های معادل و گروه های مشکل ساز در تئوری محاسبه مرتبط باشد. به طور کلی انتظار می رود که ارتباطات و پیوندهای اساسی بین تئوری محاسبه و تئوری سیستم های آماری و پیچیده نا متوازن وجود داشته باشد. تئوری اطلاعاتی تشکیل دهنده معیاری ریاضی است برای مکانیک آماری متعادل. تئوری محاسبه که با فرآیندهای زمانی سر و کار دارد نقش مهمی را در مکانیک آماری نا متوازن ایفا می کند.

۲-۹ تعریف فرمال آتوماتای سلولی

یک آتوماتای سلولی یک ماشین محاسباتی میباشد که متشکل از دو بخش فضای سلولی و قانون انتقال محلی است که هر سلول میتواند حالتهای مختلفی داشته باشد که با اندیس i مشخص میشود و حالت هر سلول در زمان t با S_i^t نشان داده میشود.

هر سلول دارای همسایگانی است که با استفاده از آنها میتوان قانون انتقال محلی را اعمال کرد و مجموعه حالت همسایگان سلول i در زمان t با η_i^t مشخص میشود و شعاع همسایگی هر سلول با r مشخص میشود.

قانون انتقال محلی تابعی از η_i^t است که روی همه سلولها بطور همزمان اعمال میشود و با $\phi(\eta_i^t)$ نشان داده میشود.

در نهایت هر آتوماتای سلولی بصورت یک چهارتایی شامل: [۱۴]

$$CA=(\Sigma,d,V,\Phi) \qquad \text{(معادله ۲-۱۱)}$$

است که داریم:

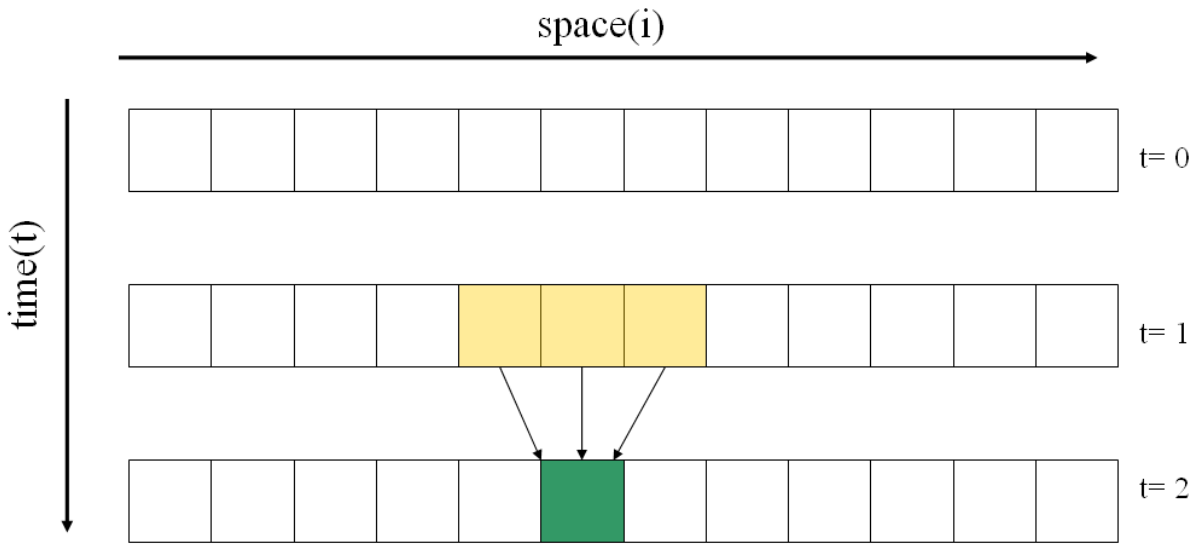
= مجموعه وضعیتهای ممکن هر سلول

d = بعد آتوماتای سلولی

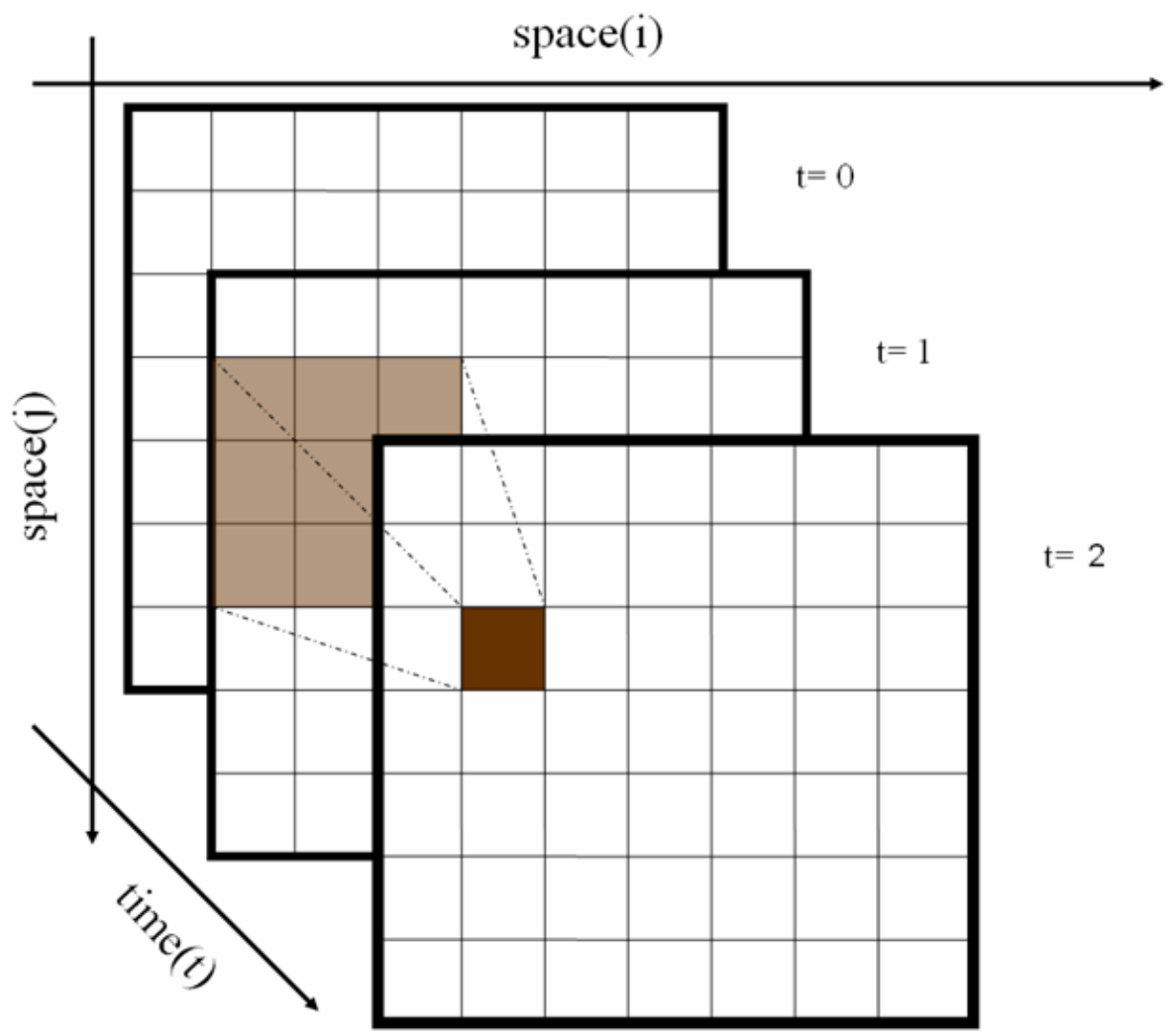
v = ساختار همسایگی آتوماتای سلولی

= قانون انتقال محلی

به عنوان مثال برای نمایش آتوماتای سلولی یک بعدی و دو بعدی داریم:



شکل ۲-۱۷: آتوماتای سلولی یک بعدی

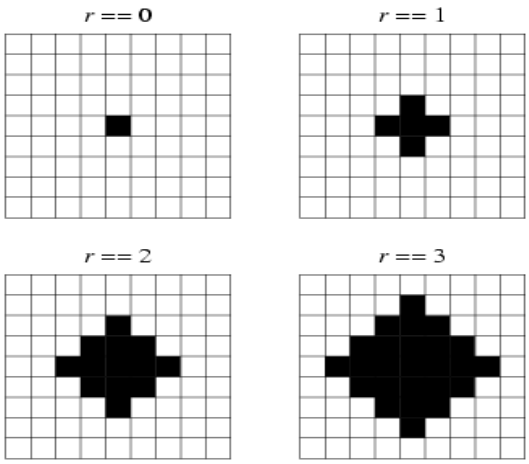


شکل ۲–۱۸: آتوماتای سلولی دو بعدی

۲–۱۰ انواع همسایگی آتوماتای سلولی

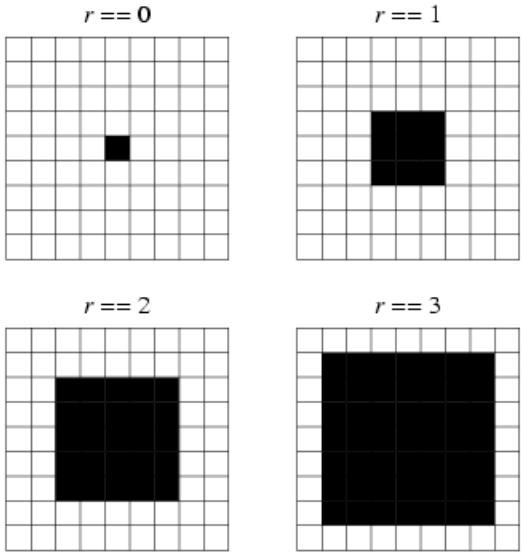
مجاورت سلولها در آتوماتای سلولی میتواند همسایگی های مختلفی ایجاد کند که از جمله معروفترین آنها میتوان به همسایگی های Von Neumann [۱۵] و Moore [۱۶] اشاره کرد.

در همسایگی Von Neumann همسایگان هر سلول فقط در جهات اصلی در نظر گرفته میشوند مانند شکل زیر:



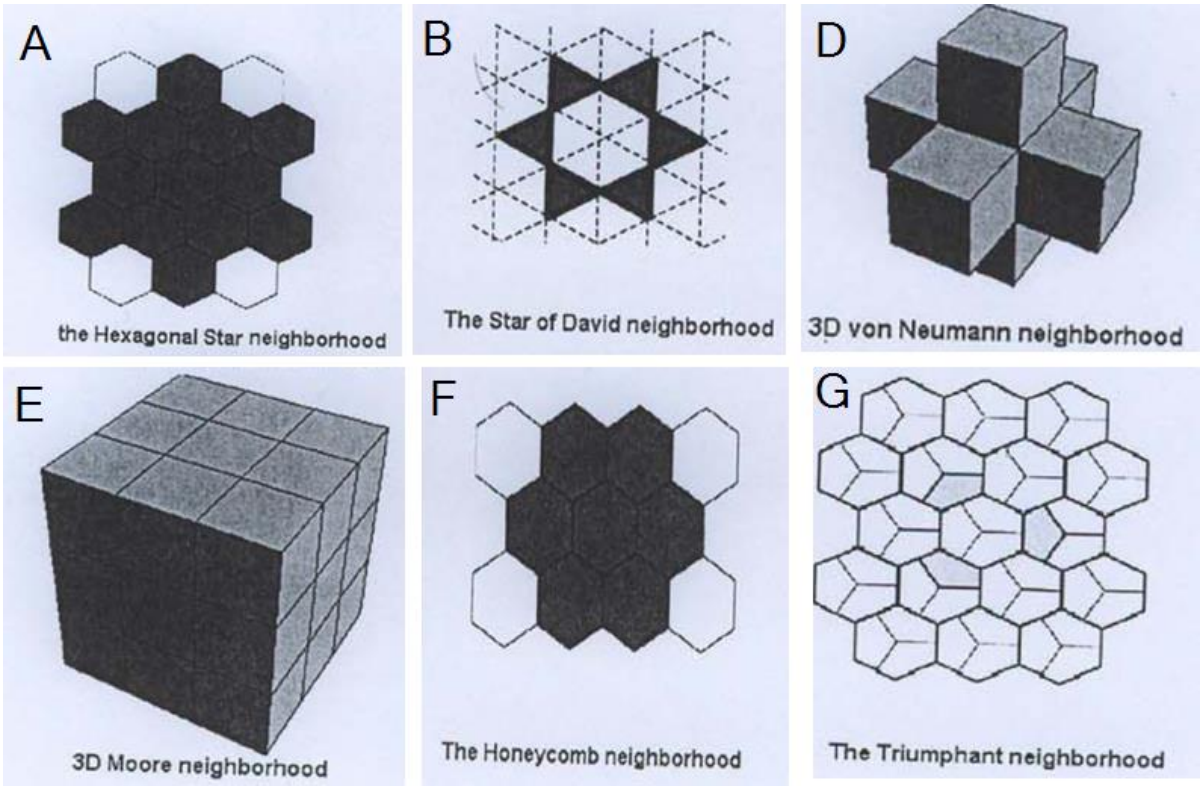
شکل ۲-۱۹: همسایگی Von Neumann در آتوماتای سلولی دو بعدی با شعاع r

ولی در همسایگی Moore همسایگان هر سلول علاوه بر جهات اصلی جهات فرعی هم در نظر گرفته میشوند مانند شکل زیر:



شکل ۲-۲۰: همسایگی Moore در آتوماتای سلولی دو بعدی با شعاع r

توجه کنید که با توجه به کاربردهای مختلف ، همسایگی های متفاوتی در آتوماتای سلولی قابل تعریف است که به عنوان مثال از معروفترین آنها میتوان به موارد زیر اشاره کرد که شکل D-۲۱ همان همسایگی Moore در آتوماتای سلولی سه بعدی است و E-۲۱ همان همسایگی Von Neumann در آتوماتای سلولی سه بعدی است.



شکل ۲-۲۱: انواع همسایگی های معروف در آتوماتای سلولی [۱۶]

۲-۱۱ انواع قوانین آتوماتای سلولی

هر آتاماتای سلولی دارای قوانین انتقال محلی است که به دو دسته Totalistic و Non-Totalistic تقسیم میشوند. [۱۷]

- قوانین Totalistic قوانینی هستند که مقدار هر سلول i در زمان t+۱ از مجموع مقادیر دیگر سلولها در زمان t بدست می آید .

به عنوان مثال برای یک آتوماتای سلولی یک بعدی داریم:

$$S_i^{t+1} = \phi[S_{i-1}^t + S_i^t + S_{i+1}^t] \qquad \text{(معادله ۲-۱۲)}$$

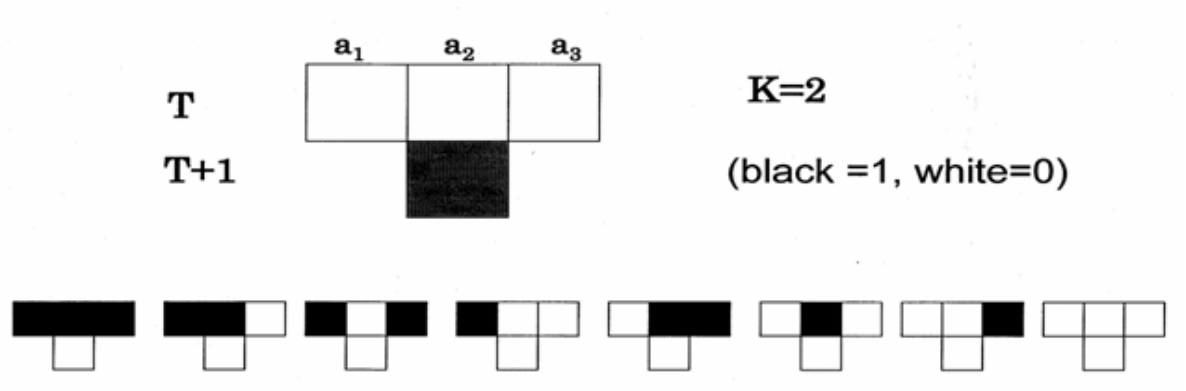
- قوانین Non-Totalistic قوانینی هستند که مقدار هر سلول i در زمان t+۱ بر اساس اعمال قانون خاصی بر دیگر سلولها در زمان t+۱ بدست می آید. به عنوان مثال برای یک آتوماتای سلولی یک بعدی داریم:

$$S_i^{t+1} = \phi[S_{i-1}^t, S_i^t, S_{i+1}^t] \qquad \text{(معادله ۲-۱۳)}$$

اگر تعداد وضعیتهای هر سلول را K و شعاع همسایگی آنرا r در نظر بگیریم تعداد عناصر در جدول قوانین k^{2r+1} میشود. به عنوان مثال برای k=۱۰ و r=۵ در جدول قوانین 10^{11} سطر و $10^{100,000,000,000}$ امکان مختلف برای آتوماتای سلولی وجود دارد در حالی که تعداد مولکولهای جهان تنها 10^{80}است.

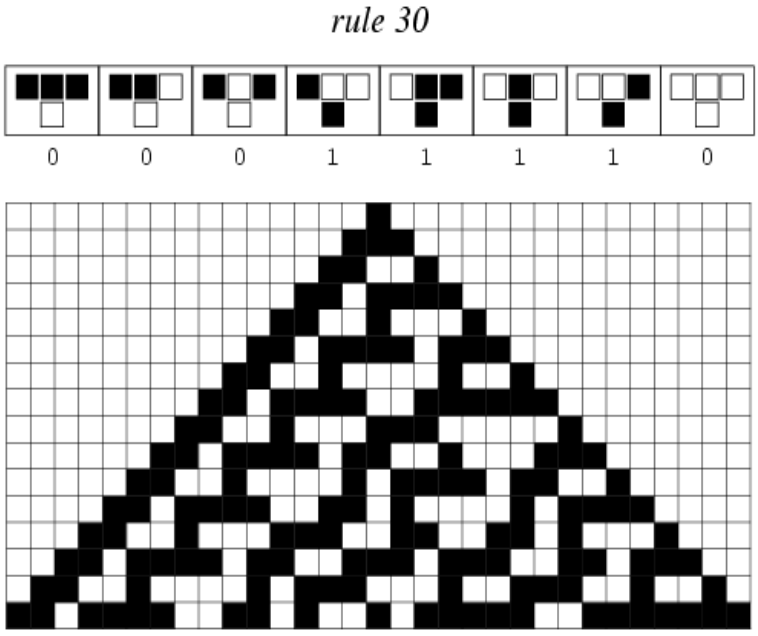
۲-۱۲ آتوماتای سلولی ساده (یک بعدی- دوحالته)

ساده ترین و متداول ترین آتوماتای سلولی ، Elementary Cellular Automata (ECA) می باشد که متشکل از تعدادی سلول که به حالت خطی در کنار هم ردیف شده اند (یک بعدی) و هر سلول دارای دو حالت {۰،۱} می باشد و تعداد حالات هر سلول k=۲ است. مانند شکل زیر:



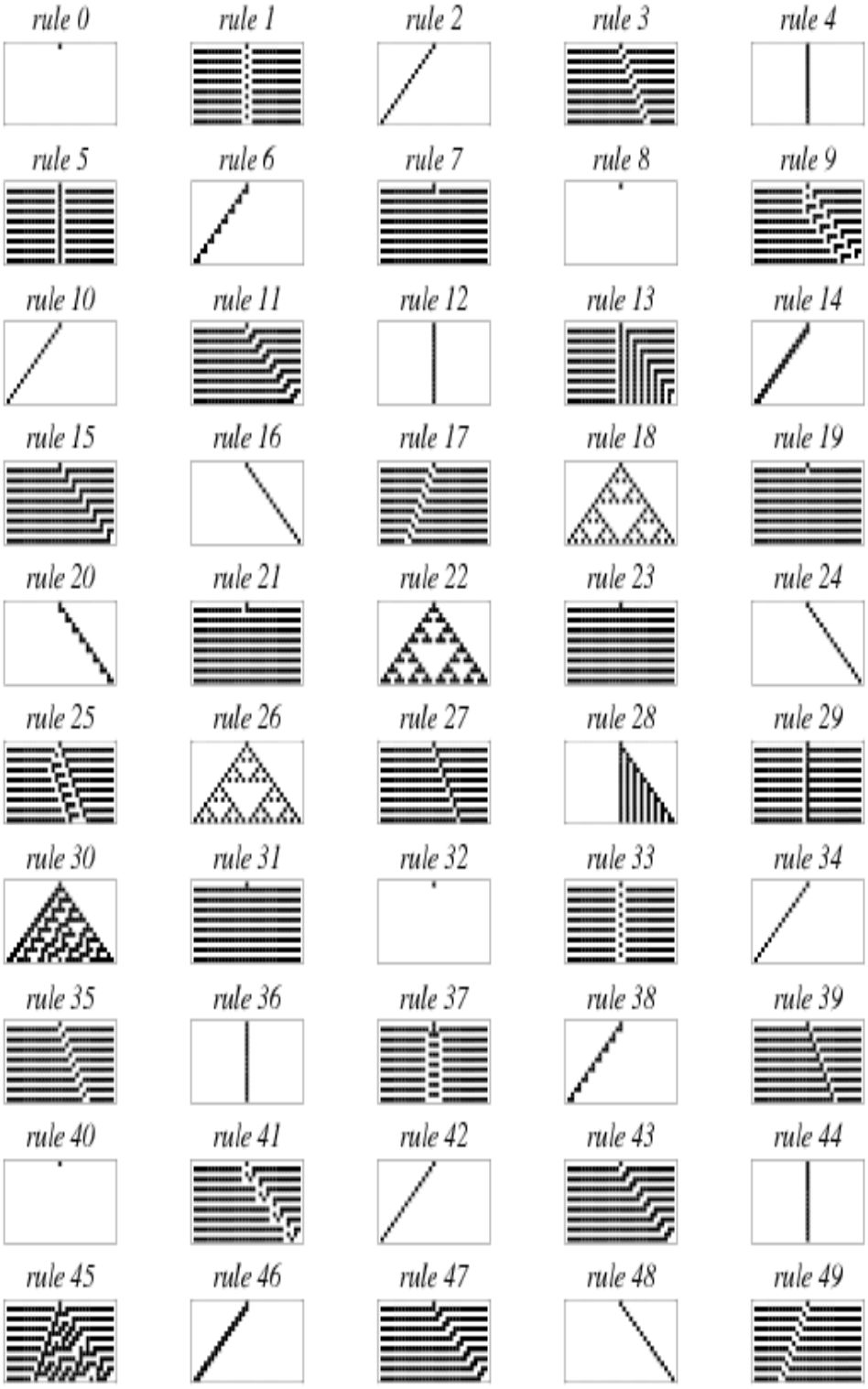
شکل ۲-۲۲: آتوماتای سلولی یک بعدی دوحالته

با توجه به شکل ۲-۲۲ تعداد ۲۵۶ عدد قانون برای آتوماتای سلولی دوحالته قابل تعریف است. بـه عنـوان مثـال بـرای قـانون ۳۰ داریم:

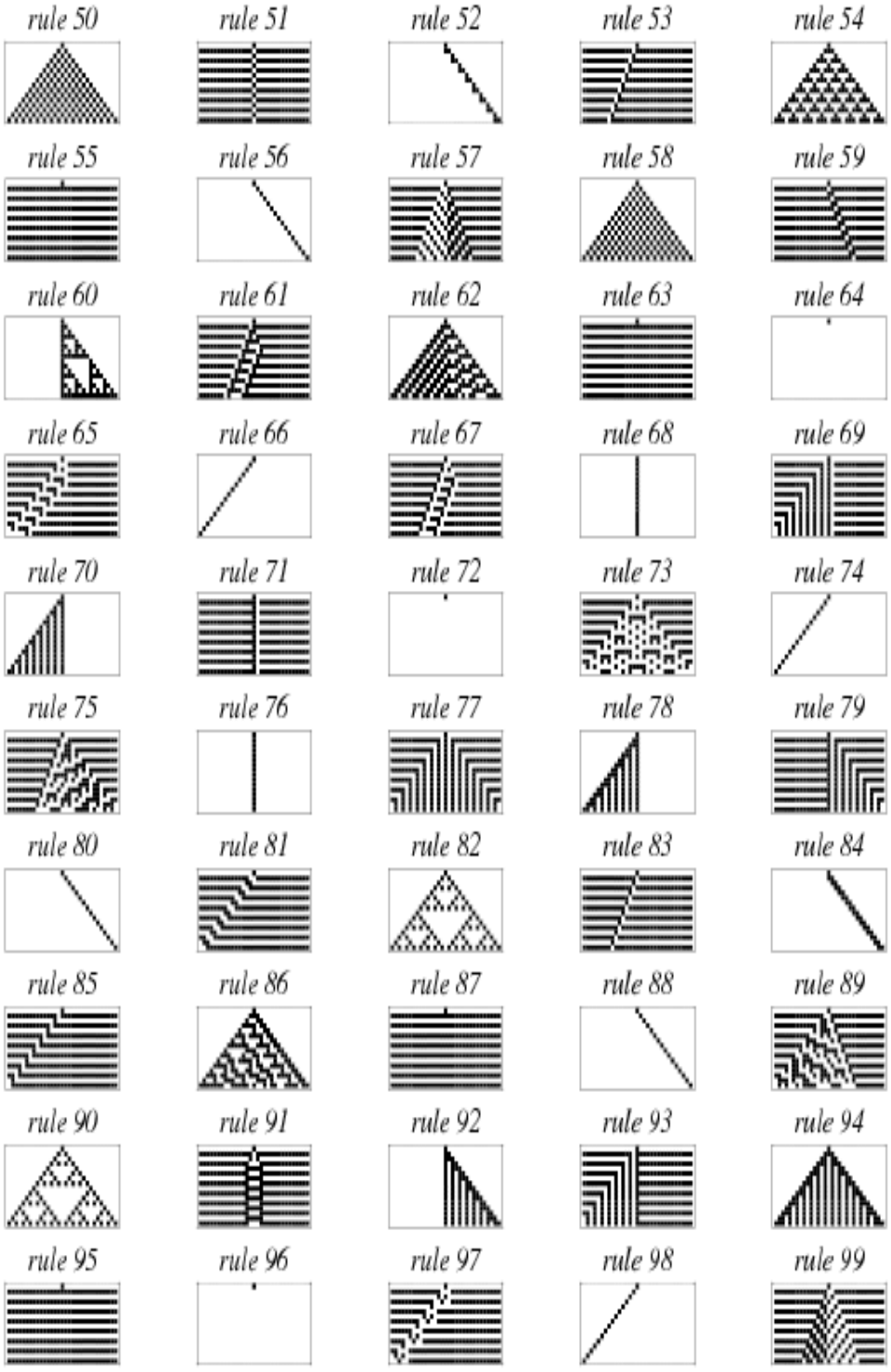


شکل ۲-۲۳: قانون ۳۰ آتوماتای سلولی یک بعدی دو حالته

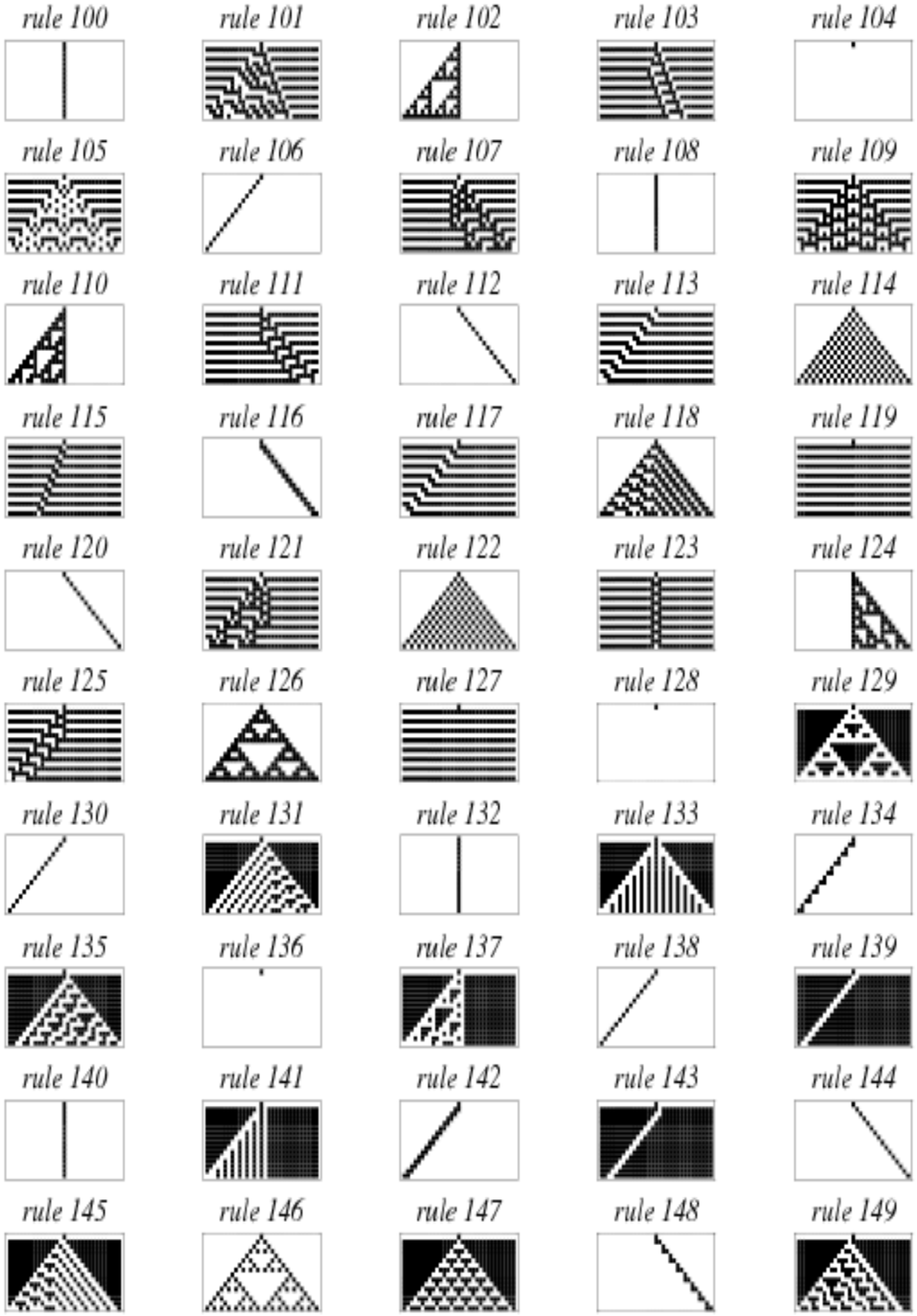
به همین ترتیب برای ۲۵۶ قانون آتوماتای سلولی یک بعدی دوحالته داریم:



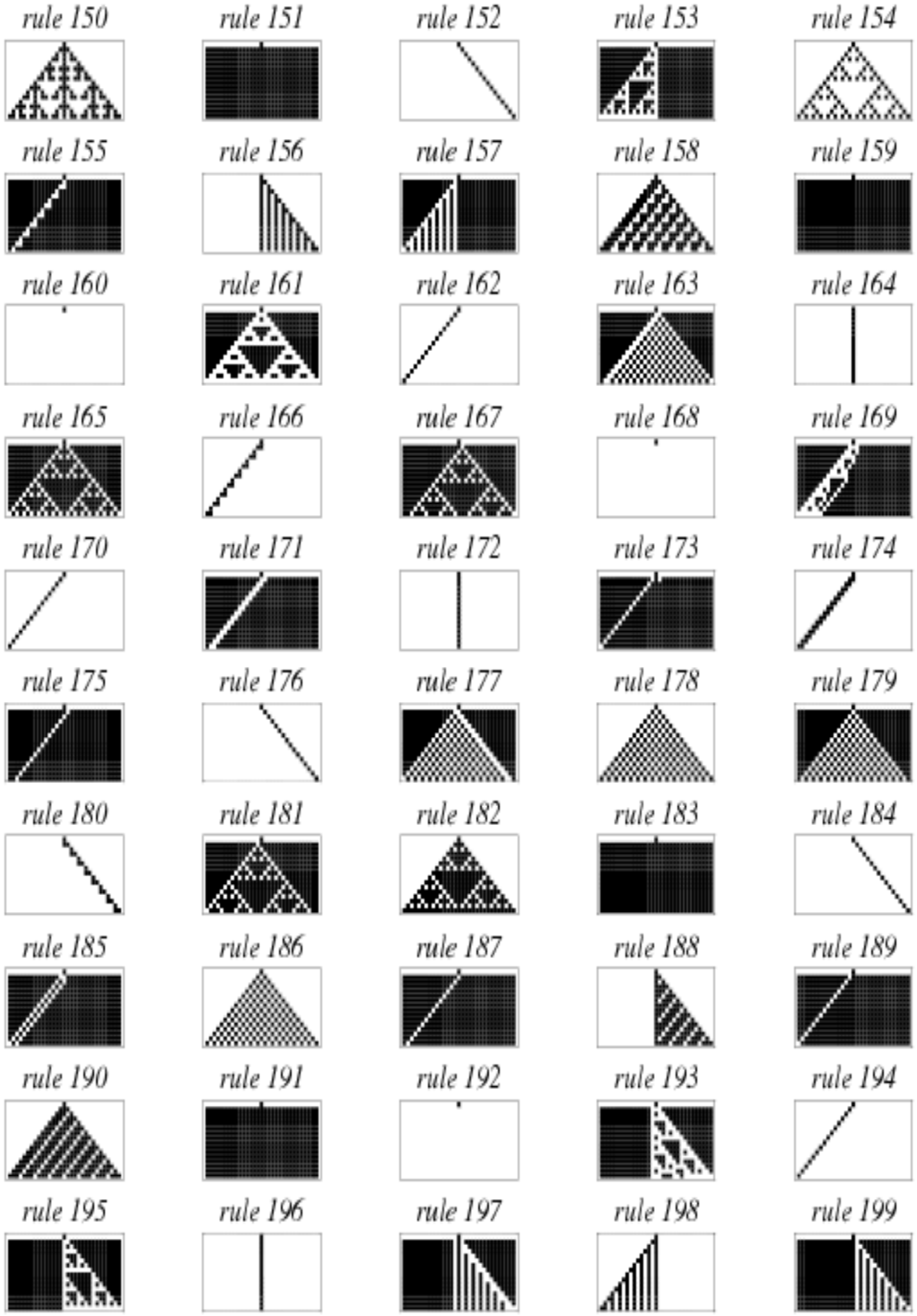
شکل ۲-۲۴: شکل حاصل از قوانین ۰ تا ۴۹ برای آتوماتای سلولی یک بعدی دوحالته



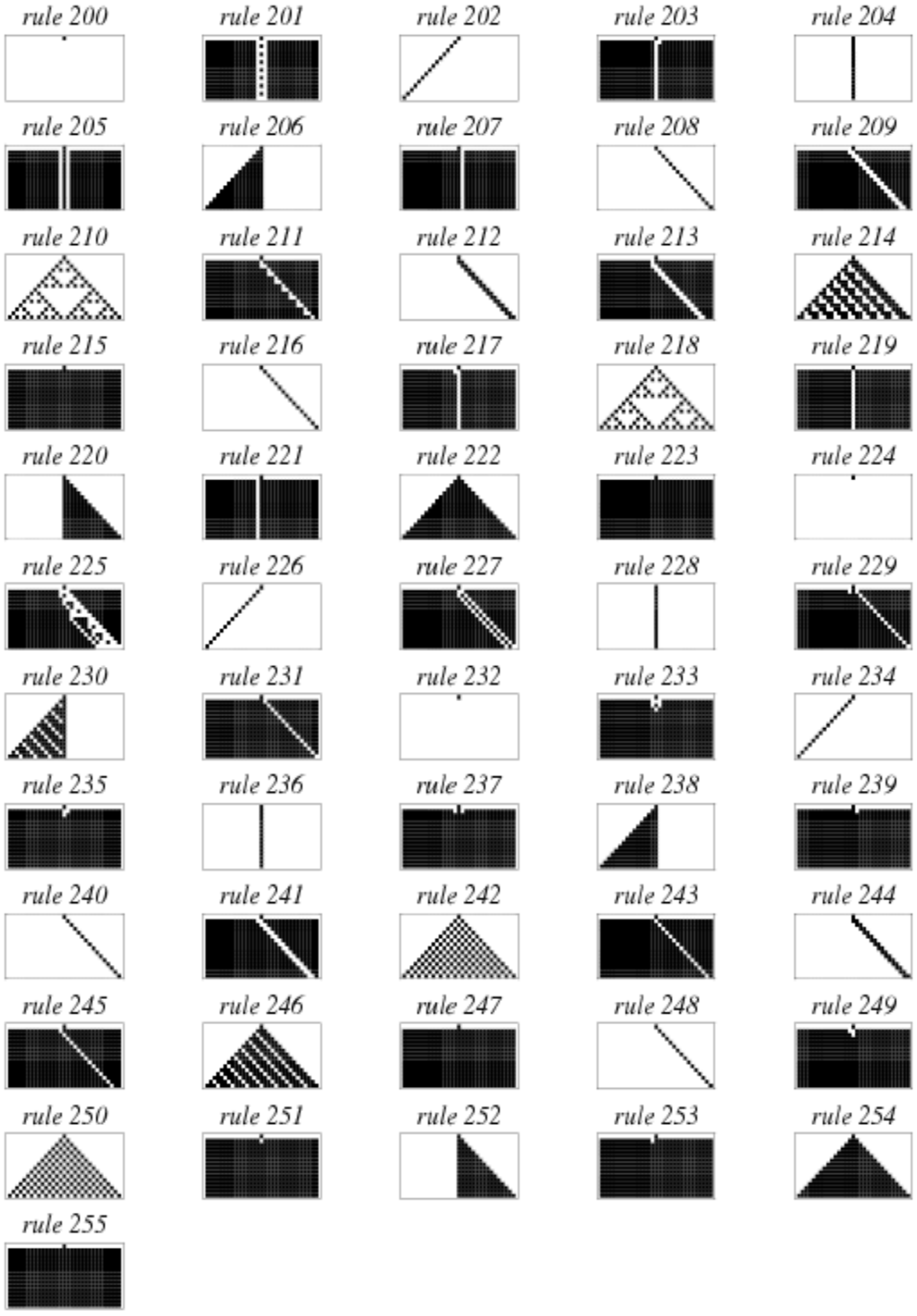
شکل ۲–۲۵: شکل حاصل از قوانین ۵۰ تا ۹۹ برای آتوماتای سلولی یک بعدی دوحالته



شکل ۲-۲۶: شکل حاصل از قوانین ۱۰۰ تا ۱۴۹ برای آتوماتای سلولی یک بعدی دوحالته



شکل ۲–۲۷: شکل حاصل از قوانین ۱۵۰ تا ۱۹۹ برای آتوماتای سلولی یک بعدی دوحالته



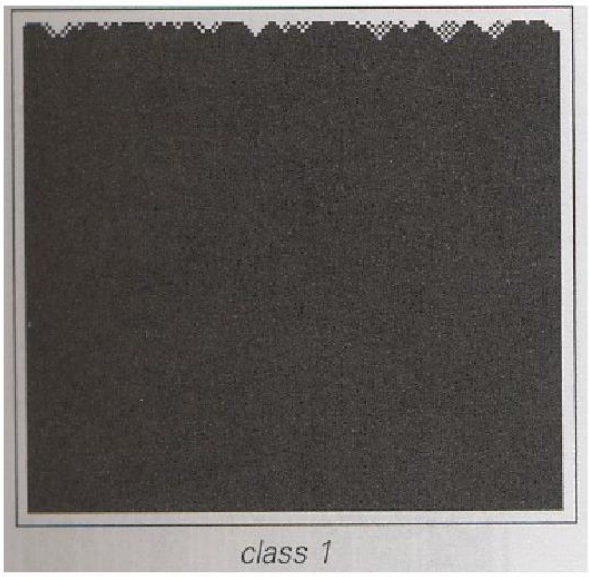
شکل ۲–۲۸: شکل حاصل از قوانین ۲۰۰ تا ۲۵۵ برای آتوماتای سلولی یک بعدی دوحالته

۲-۱۳ دسته بندی آتوماتای سلولی

انواع آتوماتای سلولی از لحاظ نوع رفتار آنها به چهار کلاس زیر تقسیم میشوند: [۱۷]

- کلاس اول Limit point :

رفتار این کلاس از آتوماتای سلولی با شروع از هر حالت اولیه به سوی یک وضعیت همگن می رود. این قوانین هرگونه اطلاعاتی را در حالت اولیه سلولها از بین می برند (شکل۲-۲۹). مثل قوانین زیر: ۰, ۳۲, ۱۲۸, ۱۶۰, ۲۵۰, ۲۵۴

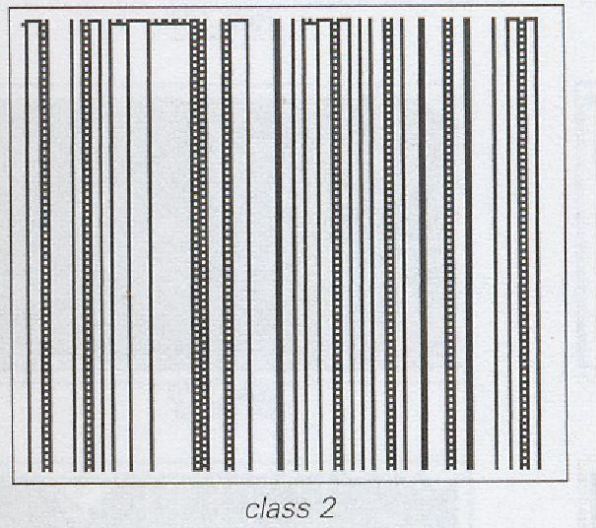


شکل ۲-۲۹: شکل حاصل از گسترش کلاس Limit point آتوماتای سلولی

- کلاس دوم limit cycle:

رفتار این کلاس از آتوماتای سلولی مثل یک فیلتر ساختارهای ساده، جدا و پریودیک می سازد (شکل۲-۳۰).

مانند قوانین :۱۳۲, ۱۶۴, ۲۱۸, ۲۲۲

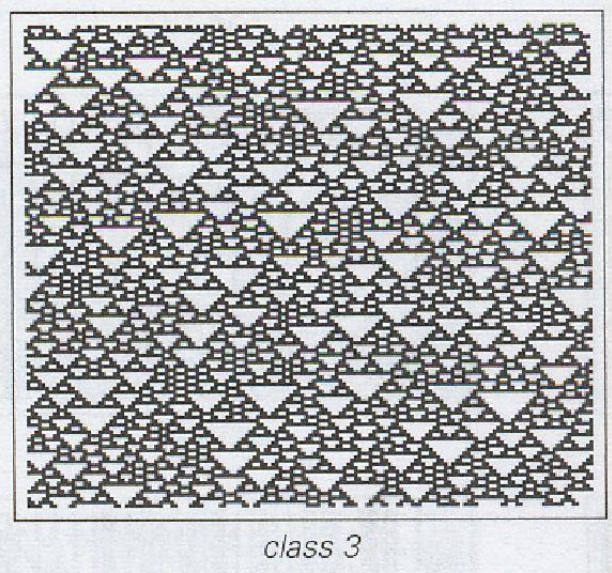


شکل ۲-۳۰: شکل حاصل از گسترش کلاس Limit cycle آتوماتای سلولی

- کلاس chaotic :

رفتار این کلاس از آتوماتای سلولی به حالتهای غیر پریودیک و غیر قابل پیش بینی از نظر فضا-زمان منجر می گردند و رفتار جالبی دارند. اکثر قوانین در این کلاس قرار دارند (شکل۳۱-۲).

مانند قوانین : ۲۲, ۳۰, ۱۲۶

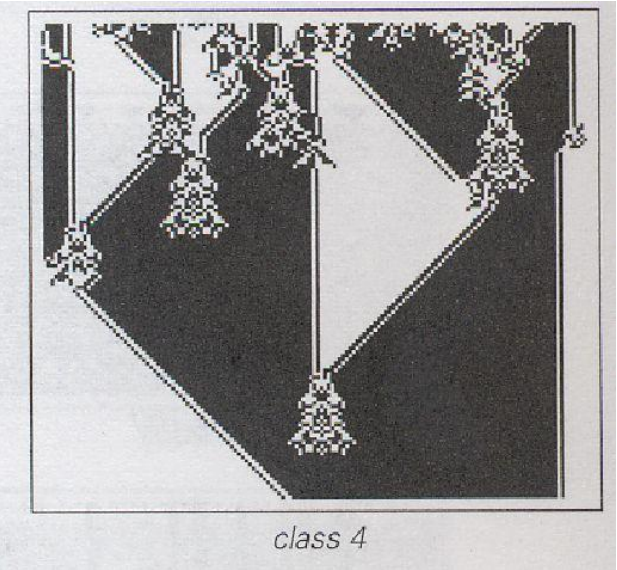


شکل ۲-۳۱: شکل حاصل از گسترش کلاس chaotic آتوماتای سلولی

- کلاس complex:

این کلاس از آتوماتای سلولی ساختارهای منتشر شونده و گاهی با عمر طولانی ایجاد می کنند. این گونه قوانین نادر هستند. این گونه قوانین دارای ویژگی عمومیت محاسبات می باشند. (شکل۲-۳۲)

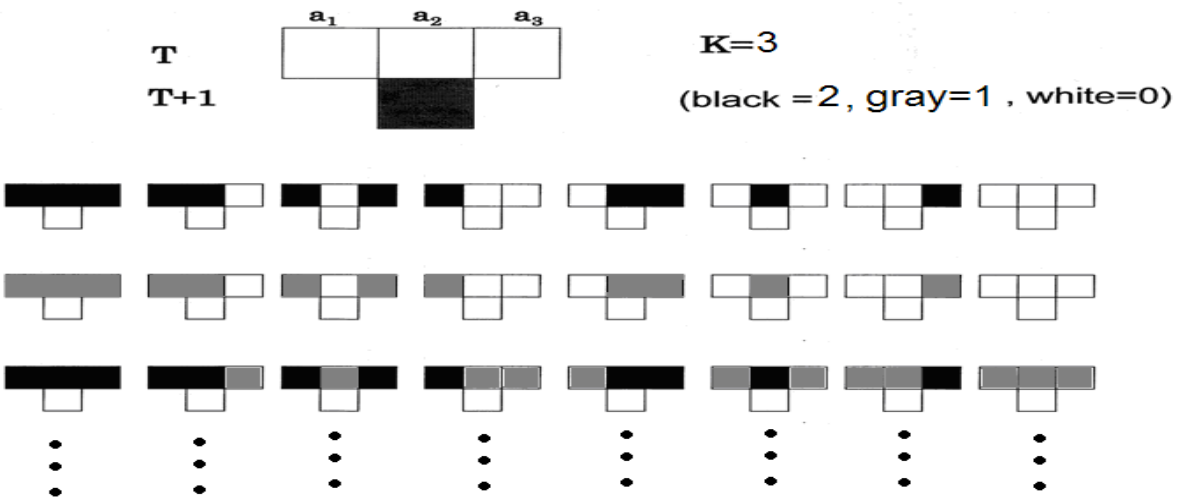
مانند قوانین زیر: ۲۰۴۳ ,۱۶۵۹ ,۲۰۰۷ ,۱۸۱۵



شکل ۲-۳۲: شکل حاصل از گسترش کلاس complex آتوماتای سلولی

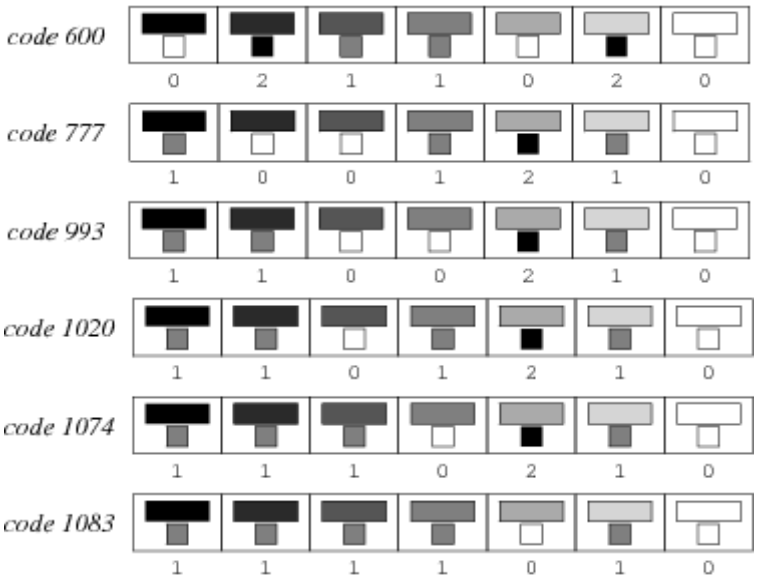
۲-۱۴ آتوماتای سلولی یک بعدی – سه حالته

در این نوع آتوماتای سلولی که متشکل از تعدادی سلول که به حالت خطی در کنار هم ردیف شده اند (یک بعدی) و هر سلول دارای سه حالت {۰،۱،۲} می باشد و تعداد حالات هر سلول k=۳ است. مانند شکل زیر:



شکل ۲-۳۳: آتوماتای سلولی یک بعدی سه حالته

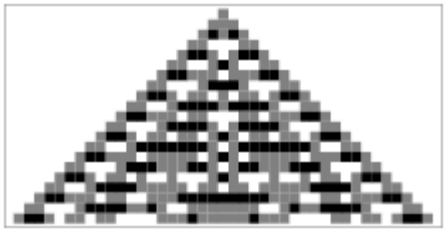
در این نوع آتوماتای سلولی تعداد 3^{27}=۷۶۲۵۵۹۷۴۸۴۹۸۷ قانون داریم که به عنوان مثال برای برخی از آنها داریم:



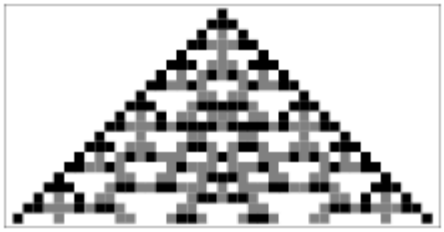
شکل ۲-۳۴: شکل جدول قوانین برخی از قوانین آتوماتای سلولی یک بعدی سه حالته

شکل حاصل از اعمال قوانین آتوماتای سلولی سه حالته و گسترش آنها بصورت زیر است:

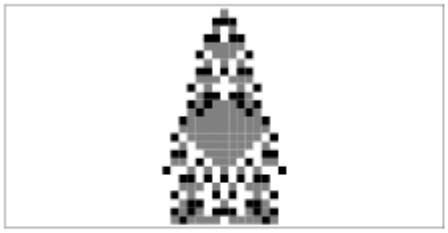
code 777



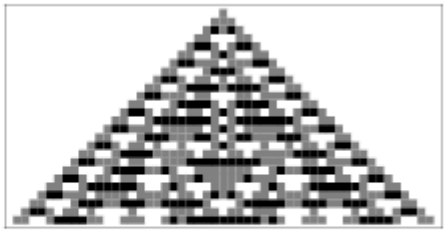
code 777



code 600

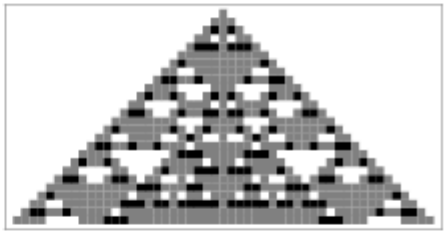


code 777



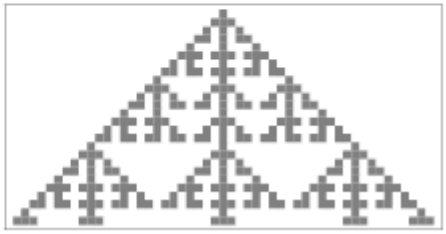
code 993

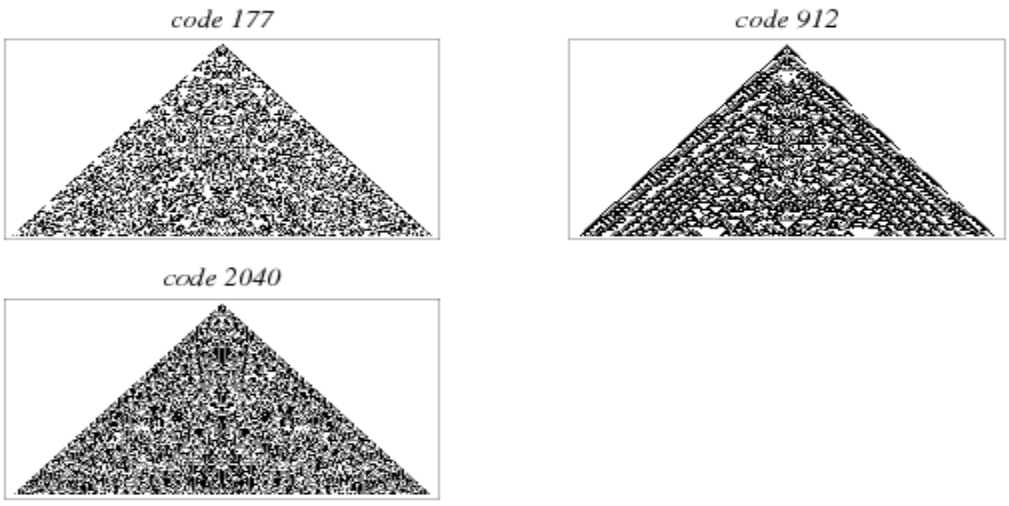
code 1020



code 1074

code 1083





شکل ۲-۳۵: شکل حاصل از گسترش برخی قوانین آتوماتای سلولی سه حالته

فصل سوم

روش پژوهش

دراین فصل به بیان روش کار با استفاده از آتاماتای سلولی برای ترکیب وب سرویس ها و افزودن امنیت به وب سرویس های مرکب با استفاده ازبسته امنیتی مبتنی بر Apache Rampart می پردازیم. برای اینکار یک بسته امنیتی با استفاده از سیاست WS-Security ساخته و تکنیک Rampart را درآن بیان می کنیم.

۳-۱ الگوریتم آتاماتای سلولی ارائه شده برای انتخاب وب سرویس های ترکیبی

الگوریتم مورد نظر در زیر بیان شده است :

```
//Uses Cellular Automata to found Rules between Quality of web services
For (i =1, i < n, i ++)
For (j =1, j < n, j ++)
}
Cin>> Availability[i][j]>>Reliability [i][j]>>Response Time[i][j]>>Cost[i][j];
Ui=∑Wj.Sij;
X=Binary (Availability[i][j] +Reliability[i][j]+ Response Time [i][j]+ Cost[i][j]+ Ui)
Rule =0, Neighborhood = VonNeumann
IF (Rule < 256)
{
 Array [Length (X)] =0
Counter = 1
IF (counter < 1000000000)
{
Y =Cellular Automata (Rule, Array, Neighborhood, Counter)
IF(Y=X)
Cout<< Rule Counter;
Else
Count = count + 1
}
Else
Rule =Rule +1;
}
Cout<<"Binary Rule Not Found";
}
}
```

شکل ۳-۱ : تولید قوانین با استفاده از آتاماتای سلولی

الگوریتم بیان شده در ادامه توضیح داده می شود:

۰. شروع

۱. دریافت Availability,Reliability,Response Time ,Cost برای ۱۰۰۰ وب سرویس مختلف

۲. تبدیل کلیه ورودی ها به مبنای ۲ و کنارهم قراردادن آنها و تولید یک عدد مبنای ۲ بزرگ

۳. درنظر گرفتن قانون صفر برای آتاماتای سلولی دوحالته

۴. درنظرگرفتن فضای سلولی به اندازه عدد مبنای ۲ بزرگ و یک حالت اولیه تصادفی برای آنها

۵. اجرای آتاماتای سلولی و اعمال قانون بر روی خانه های آن با درنظرگرفتن همسایگی VonNeumann

۶. بدست آوردن عدد مبنای ۲ بزرگ حاصل از اجرای آتاماتای سلولی بطول عدد ایجاد شده در مرحله ۲

۷. اگر عدد مبنای ۲ تولید شده در مراحل ۲ و ۶ با هم برابرند بروبه مرحله ۱۴

۸. به مرتبه تکرار یکی اضافه کن

۹. اگر مرتبه تکرار کوچکتر مساوی یک میلیارد است برو به مرحله ۵

۱۰. یکی به شماره قانون اضافه کن

۱۱. اگر شماره قانون کوچکتر مساوی ۲۵۵ است برو به مرحله ۴

۱۲. چاپ کن قانونی برای این نمونه پیدا نشد و برو به مرحله ۱۴

۱۳. قانون و مرتبه تکرار بدست آمده برای این نمونه را به عنوان خروجی چاپ کن

۱۴. پایان

بعد از اجرای این الگوریتم ویژگی های وب سرویسی که مورد نظر کاربر است باید وارد شود و تابع fitness موجود در الگوریتم برای هر وب سرویس محاسبه شود . وب سرویس های ترکیبی براساس این تابع مرتب می شوندو سپس آنهایی که کمترین مقدار را دارند انتخاب می شوند. توضیحات ذکر شده در الگوریتم زیر آمده است:

```
//An algorithm for analysis of web service selection using two-state 1-D CA
{
For (i =1, i < n, i ++)
For (j =1, j < n, j ++)
{
Cin>> Availability[i][j]>>Reliability [i][j]>>Response Time[i][j]>>Cost[i][j];
Cin>> usrAvailability[i][j]>> usrReliability [i][j]>> usrResponseTime[i][j]>>
usrCost[i][j];
X=Binary (Availability[i][j] +Reliability[i][j] + Response Time [i][j] + Cost[i][j])
IF Exist (Rule Model)
{
Rule =One of Model Rule ;
Neighborhood=VonNeumann;
Array [Length(X) + Length (Binary (Value of services[i][j]))]=o;
Counter = 1;
IF (Counter<1000000000)
{
Y=Cellular Automata (Rule, Array, Neighborhood, Counter);
Z=Partition Y from o to Length(x);
Defined Value of Web Service=Partition Y from Length(x) to Length(y);
}
IF (Z = =X)
{
Defined Value of Web Service
Fitness function [n] = Defined value web services – value services defined by
formula (1);
Find the top services with minimum Fitness function;
Top services in class i of web services;
}
Counter = Counter + 1;
}
Rule =Rule + 1;
}
```

شکل ۳-۲ : انتخاب وب سرویسها

بعد از انجام این الگوریتم بسته امنیتی نیز به وب سرویس های ترکیبی بدست آمده برای بالا بردن امنیت وب سرویس های ترکیبی اضافه می شود. درادامه این مبحث را مورد ارزیابی قرار می دهیم

۳-۲ بررسی امنیت در معماری سرویس گرا و وب سرویس ها

امروزه بهره گیری از وب سرویس ها بدون درنظر گرفتن نکات امنیتی کاری بیهوده است ، در کنار نحوه و کیفیت خدمات رسانی به مشتریان، مسائل امنیتی از مهمترین چالش های پیش روی وب سرویس ها است

نمونه هایی ازحملات علیه وب سرویس ها عبارتند از[۱۸]:

حملات DOS

حملات تزریق کد

حملات XML

و سایر ...

- حملات DOS[٤]

حمله‌ای است که باعث جلوگیری از کار یک سرویس یا مانع دسترسی به منابعی شود. به عنوان مثال حملات DOS بر روی ماشین‌های سرویس دهنده وب ممکن است منجر به این شود که سرویس دهنده قادر به سرویس دهی به مشتریان نباشد یا پر کردن پهنای باند یک ماشین باعث قطع ارتباط این ماشین با شبکه اصلی می شود.

- حملات تزریق کد

حملات تزریق کد یکی از شایعترین حملاتی است که اکثر سایت ها و وب سرویس های موجود در سطح وب نسبت به این حملات آسیب پذیر می باشند. سه نوع این حملات عبارتند از :

  - تزریق SQL (SQL injection)
  - حملات تزریق Xpath (Xpath injection)
  - حملات تزریق CSS (Cross sit scripting injection)

- حملاتSQL injection

این حمله براساس تزریق غیرمجاز SQL یک فرد از راه دور ، به یک پایگاه داده است، به گونه ای که بتوان در داده ها و جداول آن تغییر ایجاد کرد و یا به آنها دسترسی پیدا کرد. از این رو این حملات را SQL injection می نامند.

[٤] (Denial Of Service Attack)

- حملات Xpath Injection

ساختار xpath شبیه یک کوئری SQL است. Xpath یکی از تکنولوژی های مرتبط با XML می باشد که توسط W۳C استاندارد شده است xpath زبانی برای پرسش در یک سند XML براساس لیست گره های منطبق با معیارهای داده شده می باشد.

- حملات XSS Injection

این حمله که در اواخر سال ۱۹۹۹ شناخته شد، نوعی از حمله است که مهاجم کدهای مخرب خود را در برنامه کاربردی وب قرار داده و برای نفوذ به سایت ها و درواقع بازدیدکنندگان سمت مشتری استفاده می کند.به دلیل عدم دسترسی به محتوای پیام به دلیل رمزنگاری شدن آن ، فایروالهای معمولی قادر به تشخیص این نوع حملات بر روی وب سرویس ها نمی باشند. اما راهکارهای نوینی مطرح شده که با ایجاد یک فایروال اختصاصی و ایجاد یک لایه امنیتی و استقرار آن امنیت وب سرویس ها بطورموثری ارتقا می یابد.

۳-۲-۱امنیت در وب سرویس ها

سازمان ها با ورود به دنیای اطلاعات از یک طرف از امکانات و تسهیلات این شاهراه اطلاعاتی بهره مند شده و از طرف دیگر خود را درمعرض تهاجمات ناخواسته از طرف خرابکاران اینترنتی قرار می دهند. آنچه دراین میان باید درنظر داشت ، بهره گیری از امکانات اطلاعاتی موجود با توجه به اصول و استانداردهای امنیتی پیشنهادی از طرف ارگان ها و موسسات ذی صلاح است. در این میان وب سرویس ها نیز به عنوان یکی از بارزترین نمودهای معماری سرویس گرا در عصر حاضر ، از این قاعده مستثنی نبوده ، بطوریکه می بایست ضمن بهره گیری از مزایای بی شمار آن به مسائل و اصول امنیتی آن نیز توجه کافی مبذول داریم.یکی از مواردی که باید درنظر داشته باشیم این است که داده ها در شبکه درحال انتقال یا سکون هستندو داده های درحال انتقال در شبکه بین طرفین یک تبادل باید فقط و فقط توسط آنها قابل دسترسی باشند و طرف سومی قابلیت استراق سمع و جاسوسی پیام های رد وبدل شده بین دوطرف اصلی تبادل را نداشته باشد.امنیت در وب سرویس ها می تواند به دوبخش تقسیم شود[۱۹].

امنیت کانال ارتباطی بین وب سرویس ها =امنیت سطح انتقال

این بخش به ارتباط بین کاربران و فرآیندهایی مربوط می شود که احتمالا در ماشین های مختلف قرار دارند . راه کار اصلی برای تضمین امنیت ارتباطی ، کانال امن است.

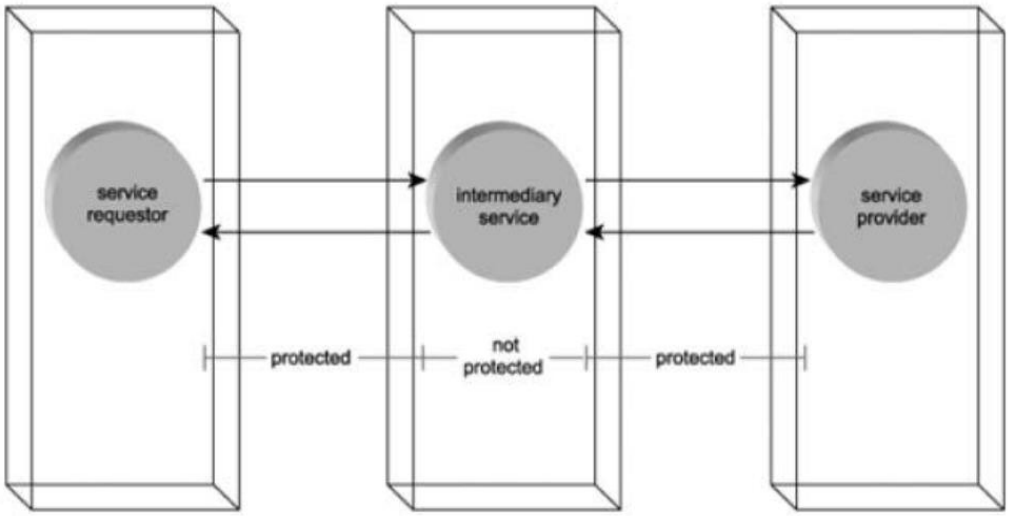
امنیت سطح پیام وب سرویس = امنیت سطح پیام

برای اطمینان یافتن از آنکه پیام بطورکامل در تمام مسیر حفاظت شده است امنیت سطح پیام نیز نیاز است

۳-۳ امنیت سطح انتقال

یک پیام در حین عبور از مسیرش باید محافظت شود. پروتکل SOAP یک بستر مبتنی برXML است که امکان تبادل داده های میان دو وب سرویس را فراهم می کند. با وجود این که پروتکل SOAP یک پروتکل ارتباطی است، اما در تامین امنیت

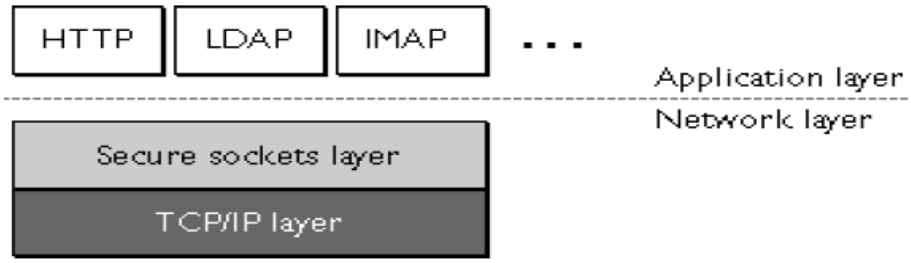
تبادل پیام نقشی ندارد. بنابراین، این ارتباط باید از یک کانال امن و با رعایت نکات امنیتی که در ادامه توضیح داده می شود،برقرار شود. شکل ۳-۳ نمایشی از امنیت در سطح انتقال را نشان می دهد.



شکل ۳-۳ : امنیت سطح انتقال

۳-۴ استفاده ازتکنولوژی امنیتی SSL وHttps

لایه اتصال امن (SSL)یک ابزار بسیار متداول برای ایمن سازی کانال های HTTP که درخواست و پاسخ ها را از طریق آن منتقل می شوند می باشد. SSL پایین تر از لایه کاربرد و بالاتر از لایه انتقال به اجرا در می آید. SSL به یک سرور با قابلیت SSL اجازه می دهد که هویت خود را به یک سرویس گیر SSLاثبات نماید .همچنین اجازه می دهد که دوطرف یک اتصال امن رمزنگاری را ایجاد نمایند و اطلاعاتشان را به صورت کد شده منتقل کنند. شکل ۳-۴ جایگاه SSL را در بین لایه های کاربرد ولایه انتقال نشان می دهد.



شکل ۳-۴: جایگاه SSL در بین دولایه کاربرد وانتقال

اگرچه تکنولوژیهای امنیتی افزوده مانند SSL و Https بخشی از مسئله را توسط رمزگذاری پیام بین دونقطه حل می کنند اما این تکنولوژی های امنیتی لایه انتقال نمی تواند امنیت انتها به انتها را بین سرویس گیرنده و وب سرویس در سیستم های توزیع شده چند لایه فراهم نماید.درواقع با چارچوب های ارتباطی مبتنی بر سرویس ، SSL تنها می تواند پیام را در انتقال بین سرویس های انتهایی (سرویس های اول و آخر که بین واسطه ای نباشد) محافظت کند. پروتوکل SSL اشکالاتی دارد که عبارتند از :

پروتکل SSL تنها امنیت نقطه به نقطه را تامین می کند.

فرض کنید قرار است یک بسته از کامپیوترA (مبدا) به کامپیوتر B (مقصد) منتقل شود.کامپیوتر A بسته را به اولین گره ارسال می کند ابتدا بسته در گره ی میانی ذخیره شده و سپس، به منظور یافتن گره ی مناسب بعدی بر روی آن پردازش هایی انجام می شود. این عمل در گره ی بعدی تکرار می شود تا زمانی که بسته به کامپیوترB ، برسد، به عبارت دیگر SSL در طی این ارتباط فقط یک کانال ارتباطی امن بین دو گره از شبکه را ایجاد می کند و نقشی در تامین امنیت مسیر بین مبدا و مقصد ندارد. بنابراین، امنیت ارتباط بین جفت گره ی {A,B} و {B,C} لزوما به معنای وجود امنیت در{A,C} نیست.

اگرچه امروزه وب سرویس هایی نیز وجود دارند که تنها با استفاده از مکانیزم SSL امنیت خود را تامین می کنند، امااین رویکرد ممکن است برای محافظت از یک برنامه ی ساده ی داخلی مناسب باشد. به منظور ایجاد امنیت بیشتر پیام ها می توان از استانداردهای مبتنی بر توکن استفاده کرد که می توانند گزینه ی مناسبی برای وب سرویس های مبتنی بر پیام باشند. استاندارد های مختلفی جهت افزایش امنیت توکن وجود دارد که در ادامه ذکر شده اند.

- پروتکل Kerberos

یک پروتکل شناسایی شبکه های کامپیوتری است که هدف اصلی آن فراهم آوردن مکانیزم شناسایی امن در مدل سرویس دهنده/سرویس گیرنده است که هم سرویس گیرنده وهم سرویس دهنده، هویت یکدیگر را از نظر صحت با دقت بسیار زیادی بررسی می کنند.

- SAML

یک استاندارد برای رمزنگاری، تصدیق اصالت و کنترل دسترسی است که در فرمت XML استفاده می شود. این استاندارد، اجازه ی تبادل اطلاعات مربوط به فرآیند تصدیق اصالت بین برنامه ها را می دهد.

- استاندارد X.۵۰۹

این استاندارد به منظور ایجاد یک شکل واحد جهانی برای صدور گواهینامه های دیجیتالی ساخته شد. طبق استاندارد X.۵۰۹ اقدام به صدور گواهینامه هایی برای اشخاص حقیقی و حقوقی یا برای یک آدرس پست الکترونیکی، آدرس DNS، یا مابقی "اشیاء" مورد حمایت این گواهینامه می کنیم.

نام کاربری و کلمه ی عبور

استفاده از نام کاربری و کلمه ی عبور نیز یکی از رایج ترین شیوه ها محسوب می شود.

امضای XML و رمزنگاری XML دو مشخصه به منظور جلوگیری از افشای داده هایXML هستند. این مشخصه ها، صحت پیام و نیز تصدیق اصالت مربوط به پیام و امضاکننده ی آن را فراهم می آورند. این امضا معادل امضای دیجیتال بوده ومی تواند برای امضا کردن اسنادXML مانند پیام های SOAP استفاده شود.

فرآیند رمزنگاری XMLامکان رمز کردن اسناد یا قسمتی از آن را فراهم می آورد. به عنوان مثال، می توان کل سند و یا خصوصیت آن که شامل محتوا، داده های غیرXML ، عاملهای XML و غیره می شود را رمزنگاری کرد.

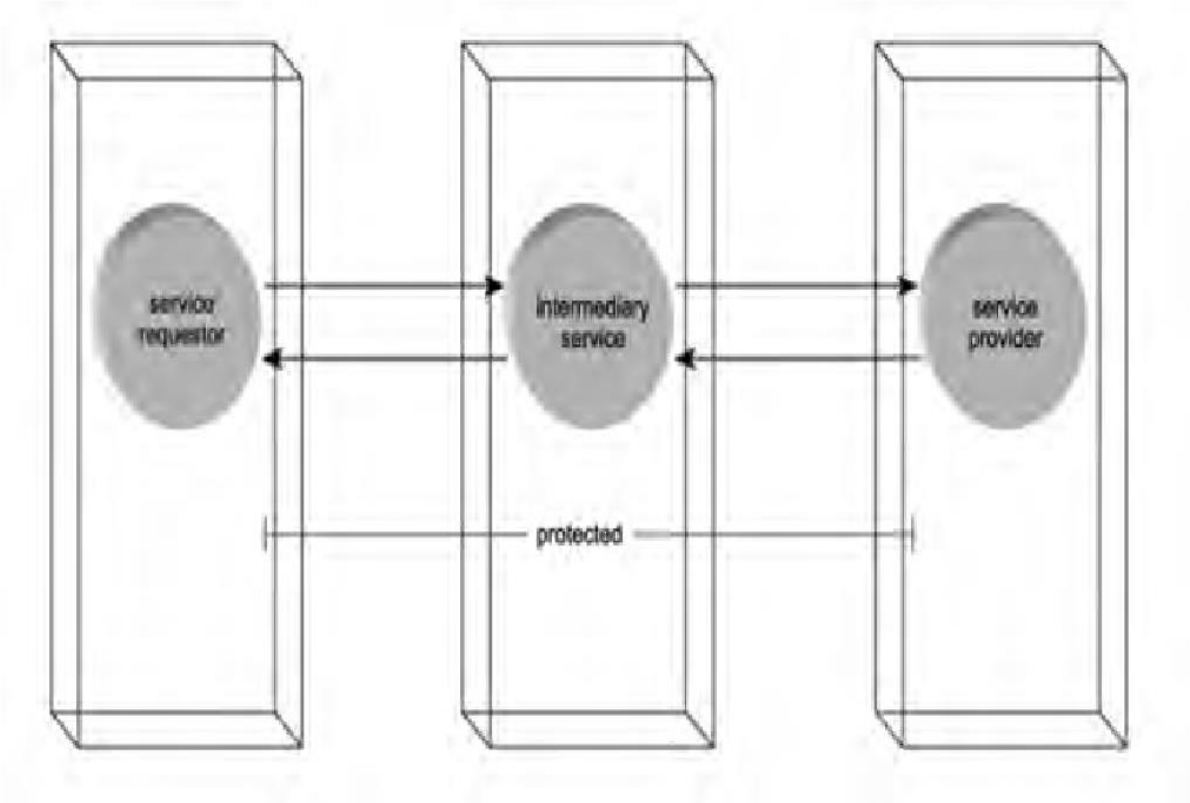
۳-۵ امنیت سطح پیام

هنگام دریافت یک پیام توسط سرویس دهنده باید دو پرسش زیر را در نظر داشت :

آیا باید به فرستنده ی پیام اطمینان کرد ؟

آیا این پیام را فرستنده ی اصلی ایجاد کرده است ؟

اگر فرض کنیم صحت فرستنده ی پیام تایید شده باشد، گام بعدی اطمینان از این موضوع است که آیا پیام مورد نظر درطول ارتباط تغییر کرده است یا نه ؟ شکل ۳-۵ نمایشی از امنیت در سطح پیام است.



شکل ۳-۵: امنیت سطح پیام

در پروتکل های ارتباطی، معمولا مکانیزم هایی مانند جمع مقابله ای جهت اطمینان از صحت پیام استفاده می شود. البته استفاده از این روش کافی نیست. در حوزه ی وب سرویس ها چنین جمع های مقابله ای به راحتی قابل تعویض هستند.

در بحث امنیت سطح پیام به دو مورد می پردازیم :

۱- استفاده از استاندارد WSS

۲- رمزگذاری وامضاهای دیجیتالی

۳-۵-۱امنیت سطح پیام(پروتوکل WSS)

برای اطمینان یافتن از آنکه پیام بطورکامل در تمام مسیر حفاظت شده است امنیت سطح پیام نیز نیاز است دراین حالت اقدامات امنیتی بر روی خود پیام اعمال می شوند نه بر روی کانال ارتباطی که پیام در آن منتقل می شود. دراین وضع صرف نظر از اینکه پیام چه مسیری را می پیماید اقدامات امنیتی نیز همراه آن هستند.برای برقرای امنیت متن پیام های وب سرویس ها که به زبان XMLهستند از رمزگذاری دیجیتال ویا از پروتوکل WSS استفاده می شود.Erl ادعا دارد که امنیت سطح پیام بعنوان مولفه اصلی راه حل های امنیت معماری سرویس گرا می باشد.

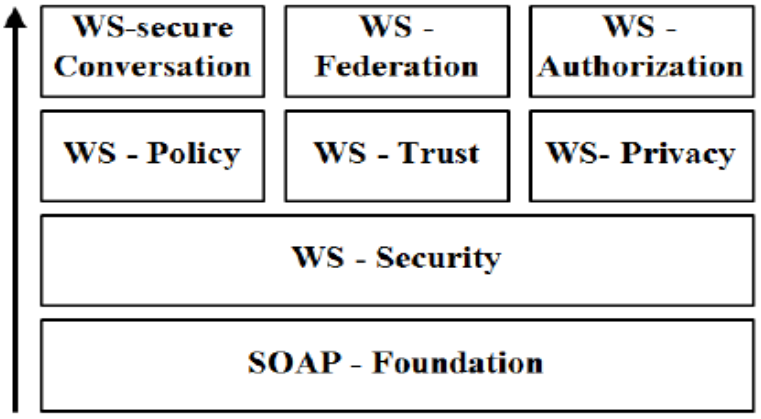
۳-۵-۱-۱ استاندارد WS-S

WSS یک پیاده سازی امنیتی است که به یک وب سرویس اضافه می شود و توسط آن پیام های SOAP رمز/ امضا می شوند و به گیرنده منتقل می شوند و رمزگشایی و راست آزمایی می شوند.اقدامات امنیتی می توانند بصورت لایه ای روی هر انتقال پیام قرار می گیرد تا از محتوای پیام محافظت کند. نکته ی قابل توجه در مورد این مشخصه این است که از استانداردهای امنیتی موجود از قبیل SAML بهره می گیرد و امکان استفاده از این استانداردها را به منظورایمن سازی پیام های وب سرویس ها فراهم می سازد.

ویژگی های امنیتی استاندارد WS-S در سرآیندهای یک پیام SOAP قرار می گیرد و کارکرد آن در لایه ی کاربردی شبکه است.این استاندارد زمینه های امنیتی زیر را برای افزایش امنیت استفاده می کند.

- روش هایی برای اضافه کردن سرآیندهای امنیتی استاندارد WS-S در بسته های SOAP
- پیوست نشانه های امنیتی و اعتبارنامه ها به پیام
- قراردادن برچسب زمان
- امضای پیام
- رمزگذاری پیام

استاندارد WSS و سایر الحاقات آن مانند WS-SecureConversation ، Ws-Federation ، WS-Policy و WS-Secure،Trust بیشتر در رابطه با امن ساختن پیام می باشند . شکل ۳-۶ نمایشی از استاندارد WSS و الحاقات مختلف آن را نشان می دهد که در ادامه به معرفی آن می پردازیم.



شکل ۳-۶ : استاندارد WSS

این الحاقات عبارتند از :

WS-secure Conversation

ارتباطات مورد اعتماد برای جلسات کاری فراهم می کند. (Security tokens) با استفاده از نشانه های امنیتی

WS-Security

مشخصه ای جامع که مجموعه ای از تکنولوژی های متداول امنیتی را تحت پوشش دارد، از جمله امضاهای دیجیتال و رمز گذاری مبتنی بر نشانه های امنیتی،شامل گواهی های X.۵۰۹

WS-Policy

به سرویس های وب امکان می دهد نیازهای خود را براساس مجموعه ای از فاکتورها بیان کنند. برای مثال سیاستگذاری یک سرویس وب می تواند شامل نیازهای امنیتی آن، نظیر رمز گذاری و امضای دیجیتال باشد.

WS-Trust

وب سرویس ها به صورت توزیع شده داده هایی را رد و بدل کرده و یا در انجام کاری با یکدیگر همکاری می کنند. به منظور همکاری این سرویس های تحت وب بایستی پروتوکلی بین آنها ایجاد شود تا ضمن حفظ امنیت بتوانند با یکدیگر همکاری کنند ، بدین منظور می توان از پروتوکل ws-Trust استفاده نمود که مدلی را برای ایجاد رابطه های اعتمادی مستقیم و غیرمستقیم به همراه واسطه را شرح می دهد.

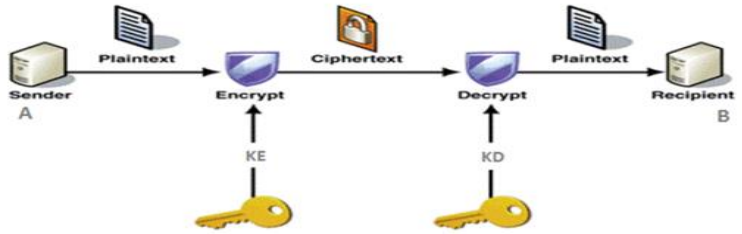
WSS معماری قابل توسعه و گسترش را برای SOAP توسط افزودن اطلاعات وابسته به امنیت مهیا می کند (نشانه های امنیتی ، امضاها و ...) این طراحی این امکان را می دهد که WSS با SOAP یکی شود. امروزه بیشتر وب سرویس ها WSS استاندارد را پشتیبانی می کنند

۳-۵-۲امنیت سطح پیام (روش رمزگذاری)

با امضای رمزنگاری شده یا کلید محرمانه ی رمزنگاری (با این فرض که کلید فقط برای دوطرف ارتباط شناخته شده است)، می توان ارتباطی امن برقرار ساخت. رمزنگاری دو جز اصلی دارد ، الگوریتم و کلید .الگوریتم یک مبدل یا فرمول ریاضی است . تعداد کمی الگوریتم قدرتمند وجود داردکه بیشتر آنها به عنوان استانداردها منتشر شده اند . کلید ، یک رشته از ارقام دودویی (صفرو یک) است که به خودی خود بی معنی است. در رمزنگاری وب سرویس فرض می کنیم که الگوریتم شناخته شده است یا می تواند کشف شود.

۳-۵-۲-۱ رمزنگاری متقارن

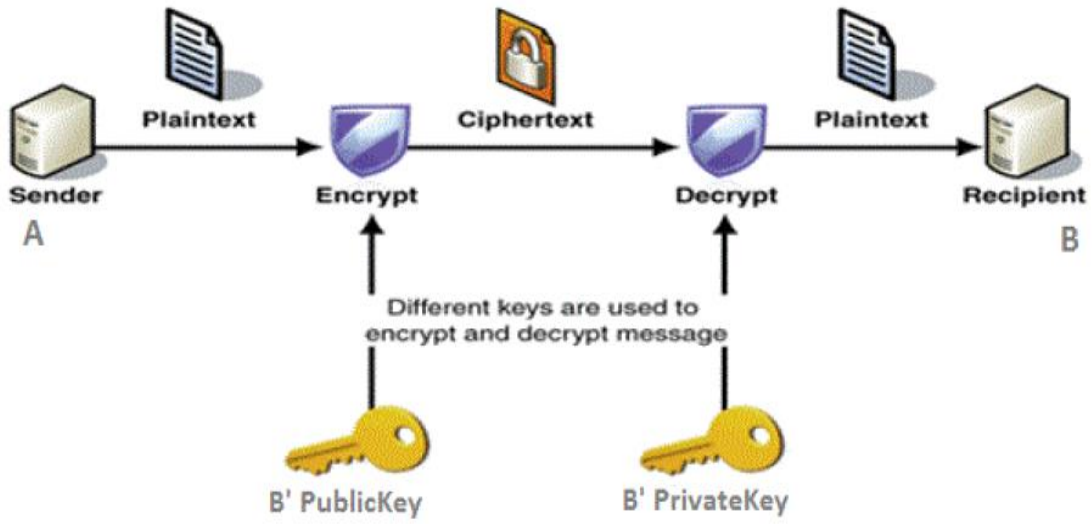
کلید رمزگشایی در سیستم های رمزنگاری متقارن یا مساوی کلید رمزنگاری است و یا به راحتی از آن استنتاج می شود. در نتیجه کافی است هر دو کاربرA, B کلید رمزنگاری را بدانند تا بتوانند پیام هایشان را توسط آن رمز کرده و سپس رمزگشایی نمایند. با توجه به این که کلید رمزنگاری تنها برای A, B شناخته شده است، لذا وقتی کاربرB پیام را باز می کند، مطمئن می شود که پیام فوق ازطرف A است (خاصیت احراز هویت) .شکل ۳-۷ الگویی از رمزنگاری متقارن اطلاعات را نشان می دهد.



شکل ۳-۷ : رمزنگاری متقارن

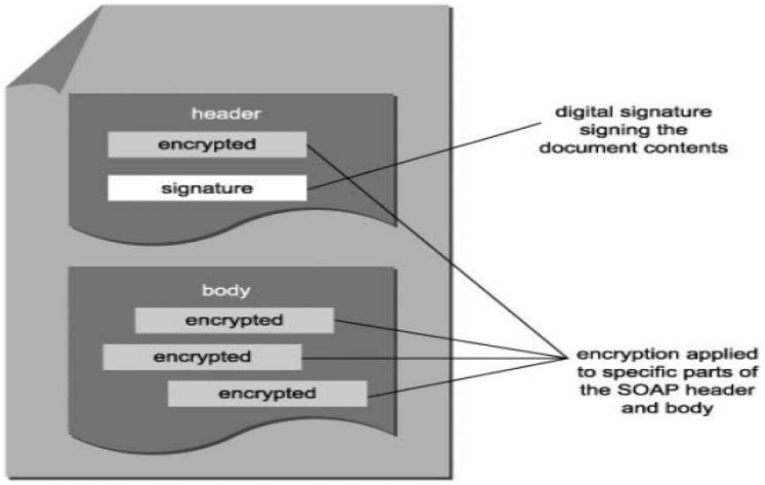
۳-۵-۲-۲ رمزنگاری نامتقارن

در سیستم های رمزنگاری نامتقارن، کلید های رمزنگاری و رمزگشایی متفاوت هستند. در حقیقت، هر کاربر دارای یک زوج کلید می باشد که یکی کلید عمومی و دیگری کلید خصوصی می باشد. کلید خصوصی، تنها توسط آن کاربرشناخته شده است، ولی کلید عمومی برای همه ی افرادی که قصد ارتباط با آن کاربر را دارند معلوم است. در واقع هرکاربر کلید خصوصی مربوط به خود را نزد خود و کلید عمومی مربوط به خود را به همه اعلام می کند. حال اگر کاربرA قصد ارسال پیامی محرمانه به کاربرB را داشته باشد، پیام را توسط کلید عمومی مربوط به کاربرB رمز می کند و آن راارسال می نماید. با توجه به این که پیام با کلید عمومی مربوط به کاربرB رمز شده است، پیام رمزنگاری شده فقط باکلید خصوصی B رمزگشایی می شود. با توجه به این که تنها کاربردارای این کلید خصوصی است، لذا هیچ فرددیگری نمی تواند به محتوای پیام دسترسی پیدا کند. شکل ۳-۸ الگویی از رمزنگاری نامتقارن اطلاعات را نشان می دهد.



شکل ۳-۸ : رمزنگاری نامتقارن

تکنولوژی رمز گذاری و امضای الکترونیکی هردوبر استفاده از کلید ها استناد دارند. (کلید اشتراکی) نیازمند آن است که هر دو گیرنده و فرستنده پیام از کلید یکسانی استفاده کنند.امضای دیجیتال اثبات می کند که یک پیام که حاوی یک سند است توسط یک درخواست کننده مشخص ارسال و به یک فراهم کننده خاص تحویل داده شده است . شکل ۳-۹ نمونه ای از یک سند دجیتالی امضا شده را نشان می دهد.



شکل ۳-۹ : سند دیجیتالی امضا شده حاوی داده های رمزگذاری شده

سیستم های کلید نامتقارن بر خلاف سیستم کلید متقارن ، از کلیدهای مخفی برای رمزنگاری و رمزگشایی استفاده می کنند. بسیاری از سیستم ها اجازه می دهند که یک جز کلید عمومی منتشر شود در حالیکه دیگر کلید اختصاصی توسط صاحبش حفظ شود. فرستنده پیام ، متن را با کلید عمومی گیرنده کد می کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری می کند. به عبارتی تنها با کلید اختصاصی گیرنده می توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی تواند به متن اصلی دست یابد ، بنابراین پیام کد شده برای هر گیرنده ای به جز گیرنده مورد نظر فرستنده بی معنی خواهد بود. معمولترین سیستم نامتقارن به عنوان RSA شناخته می شود اگرچه چندین طرح دیگر وجود دارند . می توان از یک سیستم نامتقارن برای نشان دادن اینکه فرستنده پیام همان شخصی است که ادعا می کند استفاده کرد که این عمل اصطلاحا امضا نام دارد . RSAشامل دو تبدیل است که هرکدام احتیاج به بتوان رسانی ماژولار با توان های خیلی طولانی دارد. امضا ، متن اصلی را با استفاده از کلید اختصاصی رمز می کند ، رمزگشایی عملیات مشابه ای روی متن رمزشده اما با استفاده از کلید عمومی است . برای تایید امضا بررسی می کنیم که آیا این نتیجه با دیتای اولیه یکسان است ، اگر اینگونه است ، امضا توسط کلید اختصاصی متناظر رمز شده است. به بیان ساده تر چنانچه متنی از شخصی برای دیگران منتشر شود ، این متن

شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمز شده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود ، مطابقت متن حاصل و متن اصلی نشان دهنده صحت فرد فرستنده آن است ، به این ترتیب امضای فرد تصدیق می شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود. در واقع با اینکار در الگوریتم RSA از فرمول ۳-۱ استفاده می کنیم :

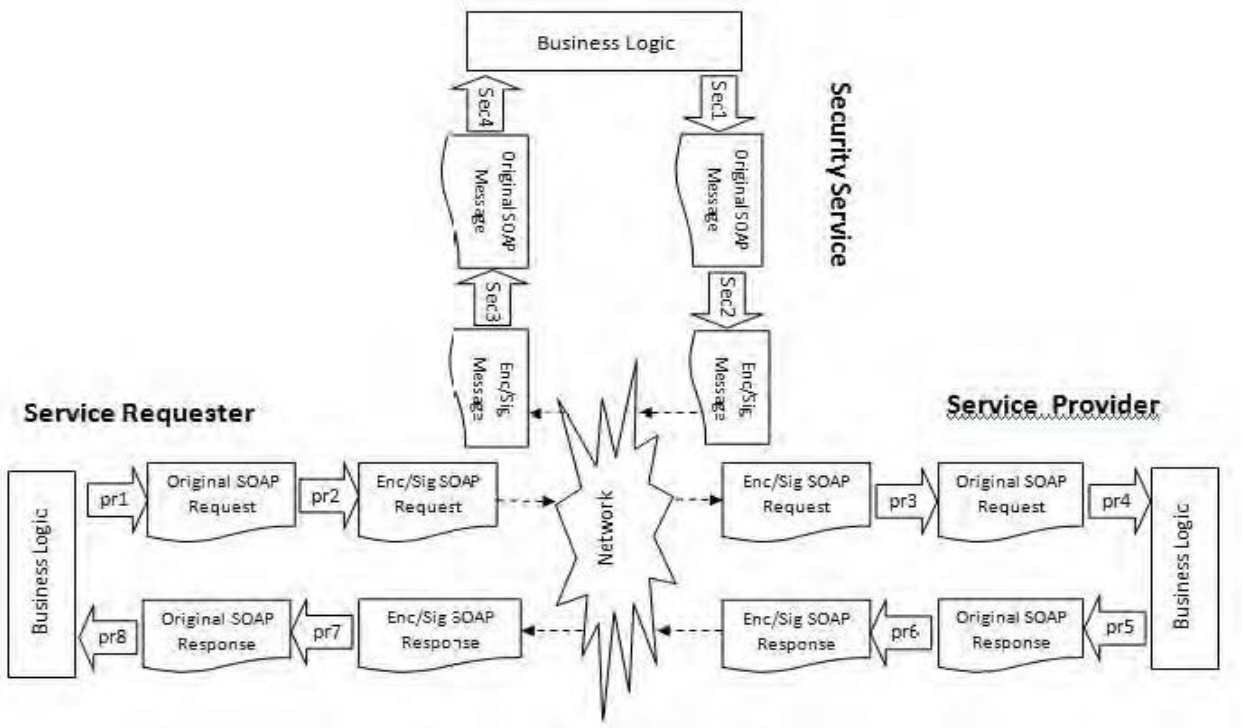
فرمول ۳-۱

$$X = YK \ (mod\ r)$$

که X متن کد شده ، Y متن اصلی ، K کلید اختصاصی وr حاصلضرب دو عدد اولیه بزرگ است که باید با دقت انتخاب بشوند. این شکل محاسبات روی پردازنده های بایتی بخصوص روی ۸ بیتی ها که در کارت های هوشمند استفاده می شود بسیار کند است. بنابراین اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن می سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارت های هوشمند الی استفاده می شود و برای نشان دادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می شود. البته خیلی از سیستم های کلید نامتقارن شامل سیستم های لگاریتم گسسته می شوند مانند Diffie-Hellman ، ELGamal و سایر طرح های چند حمله ای و منحنی های بیضوی ، بسیاری از این طرح ها عملکردهای یک طرفه ای دارند که اجازه تایید هویت را می دهند اما رمزنگاری ندارند. البته یک رقیب جدیدتر برای RSA ، الگوریتم RPK است که از یک تولید کننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می کند. RPK یک پروسه دومرحله ای دارد : بعد از فاز آماده سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی) رشته هایی از داده (دیتا) ، بطور استثنایی کار است و می تواند به راحتی در سخت افزارهای رایج پیاده سازی شود. بنابراین به خوبی بارمزنگاری و تصدیق هویت در ارتباطات سازگار است.طول کلیدها برای این طرح های جایگزین ، بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است ، که آنها را برای استفاده در چیپ کارت ها مناسبتر قرار می دهد. اما با این حال ، RSA محکی برای ارزیابی سایر الگوریتم ها باقی مانده است ، حضور و بقای نزدیک به سه دهه از این الگوریتم ، تضمینی در برابر ضعف های عمده به شمار می رود.

۳-۶ ارائه یک مدل امنیتی برای وب سرویس با استفاده از سرویس امنیتی

شکل ۳-۱۰ نحوه فراخوانی یک وب سرویس را با راهکارهای امنیتی و استفاده از یک سرویس امنیتی نشان می دهد. چهارپردازش عمده روی ماشین تقاضا دهنده ، چهارپردازش روی ماشین پاسخ دهنده ، چهار پردازش عمده روی ماشین مدیریت امنیت وجود دارد. مدیریت امنیت در این مدل امنیتی توسط یک سرویس امنیتی انجام می شود. این نوع پیاده سازی ، امنیت را به عنوان یک سرویس مستقل در نظر می گیرد و چنانچه هریک از تکنیکهای احراز هویت و توزیع نشانه و .. را خواسته باشیم استفاده می نماییم و محدودیت نخواهیم داشت. استفاده کنندگان از سرویس امنیتی می توانند بنابه سلیقه خود هرکدام از این تکنیکها را که خواسته باشند استفاده نمایند[۲۰].



شکل ۳-۱۰ : مدل امنیتی وب سرویس

Pr۱ : پروسیجرهای محاسباتی برای کدگذاری داده ها برای تولید یک درخواست SOAP ساده

Pr۲ : پروسیجرهای محاسباتی برای رمزگذاری و امضای یک درخواست SOAP ساده

Pr۳ : پروسیجرهای محاسباتی برای رمزگشایی و راستی آزمایی یک درخواست SOAP

Pr۴ : پروسیجرهای محاسباتی برای کدگشایی یک درخواست SOAP ساده

Pr۵ : پروسیجرهای محاسباتی برای کدگذاری داده ها برای تولید یک پاسخ SOAP ساده

Pr۶ : پروسیجرهای محاسباتی برای رمزگذاری و امضای یک پاسخ SOAP

Pr۷ : پروسیجرهای محاسباتی برای رمزگشایی و راستی آزمایی یک پاسخ SOAP

Pr۸ : پروسیجرهای محاسباتی برای کدگشایی یک پاسخ SOAP

Sec۱ : پروسیجرهای محاسباتی برای کدگذاری داده ها برای تولید یک پیامSOAP

Sec۲ : پروسیجرهای محاسباتی برای رمزگذاری وامضای یک پیامSOAP

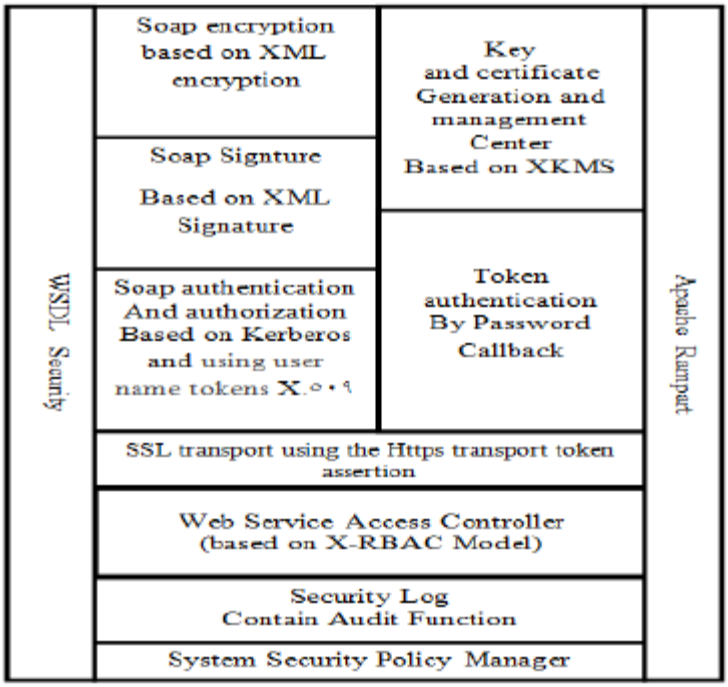
Sec۳ : پروسیجرهای محاسباتی برای رمزگشایی و راستی آزمایی یک پیامSOAP

Sec۴ : پروسیجرهای محاسباتی برای کدگشایی داده برای تولید یک پیامSOAP ساده

Pr۱ ، Pr۴ ، Pr۵ و Pr۸ پردازش های یک فراخوانی وب سرویس بدون wss هستند. Pr۲ ، Pr۳ ، Pr۶ ، Pr۷ و Sec۱ تا Sec۴ پردازشهای هستند که برای پیاده سازی امنیت در وب سرویس ها لازم هستند.

در دیدگاه سنتی، امنیت با محدود کردن مرزها و تعاملات برقرار می گردید اما از آنجایی که در معماری سرویسگرا مرزها وموانع کمتر شده، نیاز به یک بررسی مجدد در برقراری امنیت نیاز می باشد که در نهایت منجر به اضافه کردن امنیت در سطح پیام،امنیت به عنوان یک سرویس در سطح انتقال گردید. دراین پژوهش با بررسی انواع حملات به وب سرویس ها و را هکارهای های افزایش امنیت چه در سطح پیام و چه در سطح انتقالات

شبکه ای در نهایت مدلی جهت افزایش امنیت درحوزه وب سرویس و معماری سرویس گرا با استفاده از Apache Rampart مطرح شد. بسته امنیتی اضافه شده به وب سرویس های مرکب برای بالا بردن امنیت نیز مطابق با شکل ۳-۱ استفاده می شود.



شکل ۳-۱۱ :یک بسته امنیتی

۳-۷ Apache Rampart مورد استفاده در بسته امنیتی برای بالا بردن امنیت

Apache rampart یک روش بکارگیری استاندارد ws-securityبرای موتورهای وب سرویس axis۲ می باشد که توسط موسسه نرم افزاری apache استفاده شده است[۲۱]. این تکنیک از ویژگی های امنیتی مختلفی برای بالا بردن امنیت استفاده می کند. این ویژگی ها عبارتند از :

WS-Security
WS-SecurityPolicy
WS-Trust
WS-SecureConversation
SAML ۱,۱
SAML ۲,۰

تامین امنیت وب سرویس ها با استفاده از apache rampartبه صورت زیر می باشد.

- امنیت لایه انتقال

دراین بخش چگونگی استفاده از رمپارت برای افزودن امنیت به وب سرویس را در ۵ گام بررسی خواهیم کرد.

گام اول : نوشتن وب سرویس و توصیفگر وب سرویس

در اینجا یک سرویس مانند عمل add را در نظر می گیریم. این عمل دو عدد را بایکدیگر جمع کرده و یک نتیجه ای را برمی گرداند.

```
package tutorial.rampart.service;

/**
 * Secure Service implementation class
 */
public class SecureService {

    public int add(int a, int b) {
        return a+b;
    }

}
```

توصیفگر سرویس برای سرویس ذکر شده در زیر بیان شده است.

```
<service>
  <parameter name="ServiceClass" locked="false">tutorial.rampart.service.SecureService </parameter>
  <operation name="add">
    <messageReceiver class="org.apache.axis2.rpc.receivers.RPCMessageReceiver"/>
  </operation>
</service>
```

گام دوم : نوشتن وایجاد پسورد برای مخاطبین

از آنجا که برای احراز هویت و ایجاد امنیت از نام کاربری در این سناریو استفاده می کنیم نیاز به ایجاد یک کلاس برای پسورد برای مخاطبین هست تا نام های کاربری را تایید کند. اگرچه پسوردها به سختی رمزگذاری می شوند، اما به راحتی از طریق پایگاه های داده ، سرورهای LDAP یا هر محیط ذخیره سازی قابل بدست آمدن هستند. کدهای زیرفراخوانی پسوردهای مخاطبین را با Apache Rampart نشان می دهد.

```
package tutorial.rampart.service;

import org.apache.ws.security.WSPasswordCallback;

import javax.security.auth.callback.Callback;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.callback.UnsupportedCallbackException;

import java.io.IOException;

public class PWCBHandler implements CallbackHandler {

   public void handle(Callback[] callbacks) throws IOException,
        UnsupportedCallbackException {

      for (int i = 0; i < callbacks.length; i++) {

         //When the server side need to authenticate the user
         WSPasswordCallback pwcb = (WSPasswordCallback)callbacks[i];

         if(pwcb.getIdentifer().equals("apache") && pwcb.getPassword().equals("password")) {
            //If authentication successful, simply return
            return;
```

گام سوم : ساخت security policy

برای تعریف نیازمندی های وب سرویس ها باید یک security policy مناسب با استفاده از WS-Security ساخته شود.این security policy در زیر بیان شده است:

```
<wsp:Policy wsu:Id="UsernameTokenOverHTTPS" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity
        <wsp:ExactlyOne>
         <wsp:All>
            <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
             <wsp:Policy>
                <sp:TransportToken>
                 <wsp:Policy>
                    <sp:HttpsToken RequireClientCertificate="false"/>
                 </wsp:Policy>
                </sp:TransportToken>
                <sp:AlgorithmSuite>
                 <wsp:Policy>
                    <sp:Basic256/>
                 </wsp:Policy>
                </sp:AlgorithmSuite>
                <sp:Layout>
                 <wsp:Policy>
                    <sp:Lax/>
                 </wsp:Policy>
                </sp:Layout>
                <sp:IncludeTimestamp/>
             </wsp:Policy>
            </sp:TransportBinding>
            <sp:SignedSupportingTokens xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
```

گام چهارم : استفاده از rampart وبکارگیری security policy

دراین بخش به این مسئله پرداخته می شود که چگونه رمپارت به وب سرویس ملحق شده و یک security policy را ایجاد می کند. این موضوع به کمک توصیفگر سرویس بکارگرفته می شود. ما مجبور نیستیم که منبعوب سرویس را برای دسترسی به امنیت تغییردهیم بلکه در ابتدا ماژول رمپارت را با اضافه کردن <module ref = " rampart"/> به توصیفگر سرویس ، به وب سرویس اضافه می کنیم سپس با اضافه کردن policy به توضیفگر سرویس آن را امن می کنیم. توصیفگر سرویس ویرایش شده بعد از اضافه شدن رمپارت و بکار گرفتن policy در زیر بیان شده است.

```
<service>
  <module ref="rampart"/>
  <parameter name="ServiceClass" locked="false">tutorial.rampart.service.SecureService</parameter>
  <operation name="add">
    <messageReceiver class="org.apache.axis2.rpc.receivers.RPCMessageReceiver"/>
  </operation>
  <wsp:Policy wsu:Id="UsernameTokenOverHTTPS" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity
  .....
  </wsp:Policy>
</service>
```

گام پنجم : بکارگیری سرویس

اکنون ما مجبور هستیم تا این سرویس را به سرور Axis۲ اضافه کنیم. این کار با ایجاد آرشیو سرویس با نام SecureService.aar و اضافه کردن آن به دایرکتوری سرویس ها میسر خواهد شد.

وقتی یک security policy برای یک وب سرویس بکار گرفته شد WDSL با security policy های مرتبط ترکیب شده درنتیجه کلاینت با پیامهای SOAP مبتنی بر این سیاست می تواند ایمنی را افزایش دهد.

پیامهای SOAP ارسال شده با رمپارت با یکدیر ترکیب شده و security policy را ایجاد کرده است.یک هدر امنیتی به پیام SOAP اضافه شده است. در کد زیر مطلب بیان شده قابل مشاهده است:

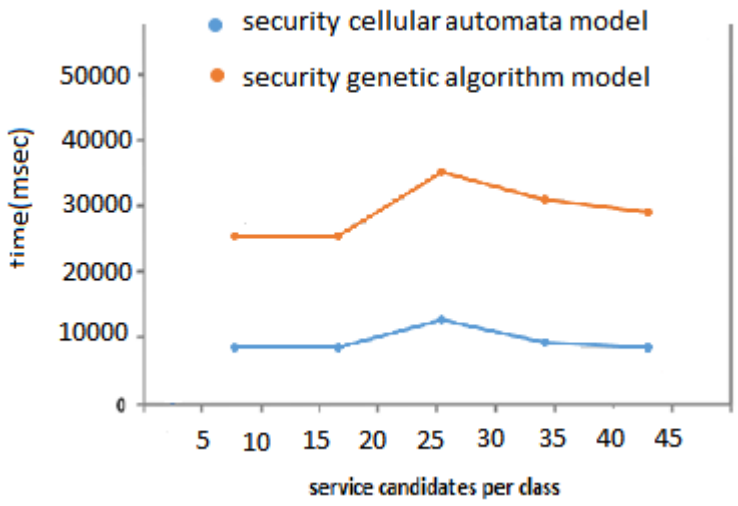
```
<soapenv:Envelope>
    <soapenv:Header>
        <wsse:Security
            soapenv:mustUnderstand="1">
            <wsu:Timestamp
                wsu:Id="Timestamp-31497899">
                <wsu:Created>2008-02-06T13:39:50.943Z</wsu:Created>
                <wsu:Expires>2008-02-06T13:44:50.943Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:UsernameToken
                wsu:Id="UsernameToken-10697954">
                <wsse:Username>apache</wsse:Username>
                <wsse:Password
                    Type="http://...#PasswordText">password</wsse:Password>
            </wsse:UsernameToken>
        </wsse:Security>
    </soapenv:Header>
    <soapenv:Body>
        <ns1:add
            xmlns:ns1="http://service.rampart.tutorial">
            <ns1:a>4</ns1:a>
            <ns1:b>6</ns1:b>
        </ns1:add>
```

باروش ذکر شده با تکنیک Apache Rampart ایمنی وب سرویس های مرکب افزایش می یابد. درادامه در فصل بعدی وب سرویس های مرکب امن با روش آتاماتای سلولی با روش های دیگر مقایسه می شود.

فصل چهارم

اطلاعات و داده ها و تحلیل آنها

روش ارائه شده در این پژوهش بر مشکلات روشهای قبلی غلبه کرده و ایده ای نوین در محاسبات وب سرویس های مرکب ایمن بیان کرده است. استفاده از روش آتاماتای سلولی که یک روش ابتکاری برای ترکیب وب سرویس ها می باشد ,برای اولین بار دراین زمینه بیان شده است و در پژوهش های قبلی وجود نداشت. استفاده از تکنیک Apache Rampart برای افزودن ایمنی به وب سرویس های مرکب نیز باعث افزایش سطح ایمنی وب سرویس ها شده است. ما الگوریتم ارائه شده در این پژوهش را با استفاده از نرم افزار JCASim شبیه سازی و مدلسازی نموده و بسته امنیتی Apache Rampart را به آن افزوده تا کارایی روش پیشنهادی را بررسی نماییم.نرم افزار JCASim یک نرم افزار همه منظوره برای شبیه سازی آتاماتای سلولی به زبان جاوا می باشد[۲۲].این نرم افزار اپلتی برای ارائه وب دارد. الگوریتم مطرح شده به صورت مرحله به مرحله به کمک این نرم افزار اجرا شده است. نتیجه حاصل نشان می دهد که برای تعداد وب سرویس های یکسان در هرکلاس روش آتاماتای سلولی ایمن مطرح شده در مقایسه با روش هایی مانند الگوریتم ژنتیک[۲۳] ایمن شده بسیار بهتر عمل کرده و در مدت زمان کمتری بهترین k وب سرویس مورد پسند برای ترکیب را انتخاب می کند. نمودار مقایسه شده این دو روش در ادامه بیان شده است.



نمودار۳-۱ : مقایسه روش آتاماتای سلولی ایمن و روش الگوریتم ژنتیک ایمن

دراین مقایسه برای تعداد ۵ ، ۱۰ ، ۱۵ ، ۲۰ ، ۲۵ ، ۳۰ ، ۳۵ ، ۴۰ و ۴۵ وب سرویس در هر کلاس مدت زمان محاسبه برای ترکیب وب سرویس ها با یکدیگر مقایسه شده است. دو الگوریتم آتاماتای سلولی و الگوریتم ژنتیک از نظر مدت زمان اجرا بایکدیگر مقایسه شده اند. نتایج نشان می دهد که الگوریتم آتاماتای سلولی سریعتر و در مدت زمان کوتاهتری اجرا شده است.

نتیجه گیری و بحث

دراین پژوهش به ارائه یک روش ابتکاری برای ترکیب وب سرویس ها پرداخته و برای بالابردن امنیت وب سرویس های مرکب از روش Apache Rampart استفاده کردیم. روش های غیرابتکاری مانند مساله کوله پشتی و روش گراف و روش های ابتکاری مانند الگوریتم ژنتیک ، الگوریتم کلونی مورچه ها ، تجمع ذرات و رقابت استعماری برای ترکیب وب سرویسها وجود دارد. دراین پژوهش سعی کرده ایم که یک الگوریتم جدید برای این مساله بیان نماییم. برای این هدف از روش آتاماتای سلولی استفاده کرده والگوریتمی مبتنی بر آتاماتای سلولی دوحالته با همسایگی VonNeumann برروی ۱۰۰۰ وب سرویس پیاده سازی کرده ایم. دریک ایده جدید برای افزودن امنیت بیشتر به وب سرویس های مرکب از روش Apache Rampart استفاده کرده و دریک بسته امنیتی آن را به وب سرویس های مرکب اضافه کرده ایم. سپس با استفاده از نرم افزار JCASim به مدلسازی و شبیه سازی الگوریتم ارائه شده پرداخته و نتایج بدست آمده را با روش های ابتکاری موجود مانند الگوریتم ژنتیک مقایسه کرده ایم. نتایج حاکی از این بود که الگوریتم ارائه شده بسیار سریعتر و در مدت زمان کوتاهتری به ترکیب وب سرویس های مرکب نسبت به سایر روشها می پردازد.

مراجع :

١. Yong-Yi Fanjiang, Yang Syu, Jong-Yih Kuo, Search based approach to forecasting QoS attributes of web services using genetic programming, Information and Software Technology, Volume ٨٠, December ٢٠١٦, Pages ١٥٨-١٧٤.

٢. Alan De Renzis, Martin Garriga, Andres Flores, Alejandra Cechich, Alejandro Zunino, Case-based Reasoning for Web Service Discovery and Selection, Electronic Notes in Theoretical Computer Science, Volume ٣٢١, ٢٠١٦, Pages ٨٩-١١٢

٣. Hanine Tout, Azzam Mourad, Chamseddine Talhi, Hadi Otrok, AOMD approach for context-adaptable and conflict-free Web services composition, Computers & Electrical Engineering, Volume ٤٤, May ٢٠١٥, Pages ٢٠٠-٢١٧.

٤. Fatih Karatas, Lars Fischer, Dogan Kesdogan, Service composition with consideration of interdependent security objectives, Science of Computer Programming, Volume ٩٧, Part ٢, ١ January ٢٠١٥, Pages ١٨٣-٢٠١.

٥. Gopal N. Rai, G.R. Gangadharan, Vineet Padmanabhan, Algebraic Modeling and Verification of Web Service Composition, Procedia Computer Science, Volume ٥٢, ٢٠١٥, Pages ٦٧٥-٦٧٩.

٦. Dandan Wang, Yang Yang, Zhenqiang Mi, A genetic-based approach to web service composition in geo-distributed cloud environment, Computers & Electrical Engineering, Volume ٤٣, April ٢٠١٥, Pages ١٢٩-١٤١.

٧. Zinoviev A, O. Zinovieva, V. Ploshikhin, V. Romanova, R. Balokhonov, Evolution of grain structure during laser additive manufacturing. Simulation by a cellular automata method, Materials & Design, Volume ١٠٦, ١٥ September ٢٠١٦, Pages ٣٢١-٣٢٩.

٨. Michele Guidolin, Albert S. Chen, Bidur Ghimire, Edward C. Keedwell, Slobodan Djordjević, Dragan A. Savić, A weighted cellular automata ٢D inundation model for rapid flood analysis, Environmental Modelling & Software, Volume ٨٤, October ٢٠١٦, Pages ٣٧٨-٣٩٤.

٩. Selman Uguz, Hasan Akin, Irfan Siap, Ugur Sahin, On the irreversibility of Moore cellular automata over the ternary field and image application, Applied Mathematical Modelling, Volume ٤٠, Issues ١٧–١٨, September ٢٠١٦, Pages ٨٠١٧-٨٠٣٢.

١٠. Mateusz Sitko, Maciej Pietrzyk, Lukasz Madej, Time and length scale issues in numerical modelling of dynamic recrystallization based on the multi space cellular automata method, Journal of Computational Science, Volume ١٦, September ٢٠١٦, Pages ٩٨-١١٣.

١١. Kechaidou M.G, Sirakoulis G.CH, Game of Life variations for image scrambling, Journal of Computational Science, Available online ٩ September ٢٠١٦.

١٢. Mousumi Saha, Mamata Dalui, Biplab K Sikdar, A cellular automata based highly accurate memory test hardware realizing March C−, Microelectronics Journal, Volume ٥٢, June ٢٠١٦, Pages ٩١-١٠٣.

١٣. Ugur Sahin, Selman Uguz, Hasan Akın, Irfan Siap, Three-state von Neumann cellular automata and pattern generation, Applied Mathematical Modelling, Volume ٣٩, Issue ٧, ١ April ٢٠١٥, Pages ٢٠٠٣-٢٠٢٤.

١٤. Moore and Hahn. Multilocus Pattern Recognition using Cellular Automata and Parallel Genetic Algorithms.In Proc. of the Genetic and Evolutionary Computation Conference .

١٥. Yingqing He, Bin Ai, Yao Yao, Fajun Zhong, Deriving urban dynamic evolution rules from self-adaptive cellular automata with multi-temporal remote sensing images, International Journal of Applied Earth Observation and Geoinformation, Volume ٣٨, June ٢٠١٥, Pages ١٦٤-١٧٤.

١٦. Moore and Hahn. A Cellular Automata-based Pattern Recognition Approach for Identifying Gene-Gene and Gene-Environment Interactions.American Journal of Human Genetics.

١٧. Wolfram. Statistical Mechanics of Cellular Automata. Rev. Mod. Phys.,٢٠١٠.

١٨. Cheng Huang, JiaYong Liu, Yong Fang, Zheng Zuo, A study on Web security incidents in China by analyzing vulnerability disclosure platforms, Computers & Security, Volume ٥٨, May ٢٠١٦, Pages ٤٧-٦٢.

١٩. Yesiltepe, M. and O. Osgur. Security Type Comparison In Service Oriented Architecture Security. in World Conference on Technology, Innovation and Entrepreneurship. ٢٠١٥.

٢٠. Wang, S. and Y. Gong, *Service vulnerability scanning based on service-oriented architecture in Web service environments.* Journal of Systems Architecture, ٢٠١٣. ٥٩(٩): p. ٧٣١–٧٣٩.

٢١. Bocciarelli, P. and A. Ambrogio, *A model-driven method for the design-time performance analysis of service-oriented software systems*, in *Modeling and Simulation of Computer Networks and Systems*. ٢٠١٥. p. ٤٢٥–٤٥٠.

٢٢. Uwe Freiwald, Jörg R. Weimar, The Java based cellular automata simulation system—JCASim, Future Generation Computer Systems, Volume ١٨, Issue ٧, August ٢٠٠٢, Pages ٩٩٥-١٠٠٤

٢٣. Mardukhi. F, Nematbakhsh. N, Zamanifar. K, Barati. A, "QoS Decomposition for Service Composition Using Genetic Algorithm, " Journal of Applied Soft Computing, Vol. ٣, Issue ٧, Pages ٣٤٠٩-٣٤٢١, July ٢٠١٣, Elsevier.

ABSTRACT

Web services are modular, comprehensive, independent, and reusable that easy business transactions in distributed environments.Todays Web services are one of the most important groups use service-oriented architecture.Web service is a software that provide access to information and information processing systems apart from distributed hardware and Mass using standard Internet provides information.Currently, security is the biggest barrier to web development service level up efforts have been made in the field of web services that include standard protocols and technologies to meet the needs in the field of Web Security Service.It sometimes a Web service can not be used and it is necessary to make a request multiple services.The process of combining several Web services are called web service composition.One of the challenges in web service composition, selecting a web service.Due to the large number of Web Services in distributed environments Choose Web services plays an important role in Web service composition.Web services that are candidates to do a job of work desired operational characteristics are the same as they do, but in terms of qualitative characteristics are different.So choosing a web service based on quality attributes is a significant problem in distributed systems.users tend to choose a service that will meet their needs This project focused on Web services selection and Web services security based on Apache Rampart And present a new approach to composition and selection of web services using artificial intelligence techniques such as cellular automata.A cellular automata is a computing machine composed of two parts, the cellular space and local transport lawthat each cell can have different states and state of each cell is determined by the index i at time t is shown.Each cell has neighbors that their use can be applied to local transport law And mode of cell i at time t is determined neighbors and the neighbors of each cell radius r is determined.Each cellular automata included:

$CA = (\sum , d , V, \Phi)$

$\sum$: Possible states of a cell
D : Cellular automata dimention
V : The structure of the vicinity of cellular automata
Φ : Local transport Rule

Ministry of Science, Research and Technology

Payam Noor University

Security in Web Service Composition

By:

Afsaneh Banaitalebi Dehkordi

Date:

October۲۰۱۶