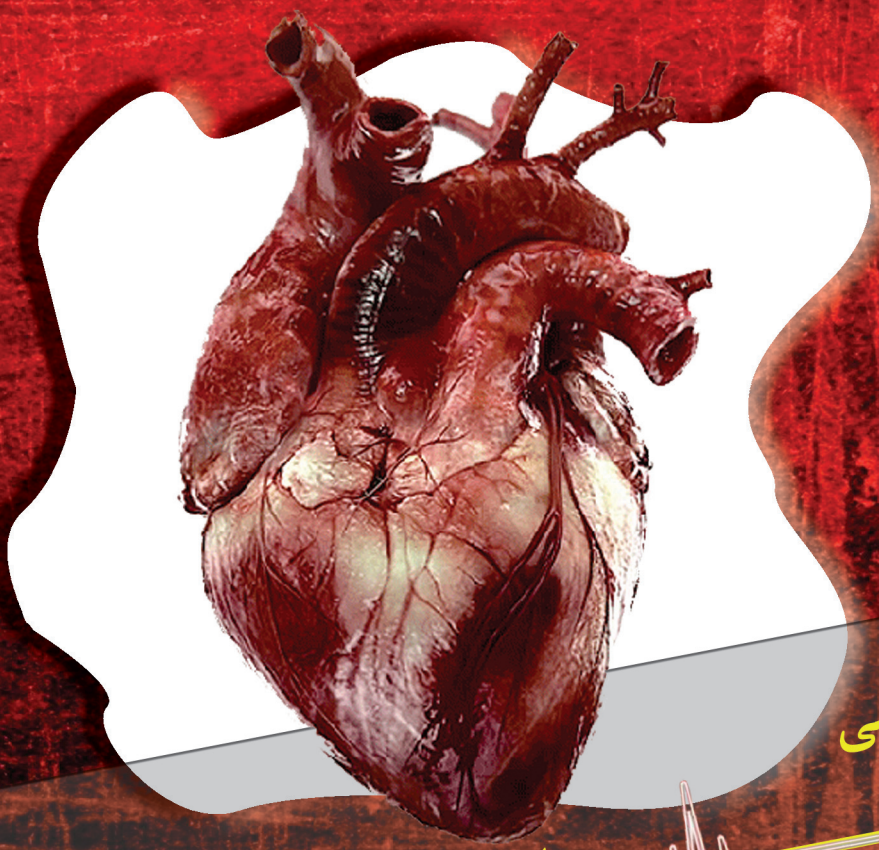
رادیکال ۲

نشریه علمی-تخصصی-دانشجویی ریاضی دانشگاه الزهراء (س)
شماره دوازدهم
پاییز و زمستان ۹۳
۱۰۰۰ تومان



تحلیل ریاضی
نوای قلب

مصاحبه اختصاصی با آقای دکتر سعید رنجبر

معرفی اپلیکیشن تد
رمزنگاری کافی نیست!
حل تقریبی معادلات انتگرال آبل
منطق بن و توسعه های آن
پالیندروم چیست؟

رادیکال ۲

نشریه علمی- دانشجویی
رادیکال ۲
پاییز و زمستان ۹۳- شماره ۱۳

رادیکال ۲

آدرس
تهران، میدان ونک، خیابان شیخ بهایی، دانشگاه الزهرا(س)

Email:
mahnamzaman@yahoo.com
maryam_bahary_۱۹۹۲@yahoo.com

بسم الله الرحمن الرحیم

نون والقلم و ما یسطرون
سوگند به قلم و آنچه
که می نویسد

تقریبا اواسط کلاس بود و همه تندتند در حال نوشتن بودند .استاد در حال قدم زدن چند لحظه ای کنار پنجره ایستادند و به منظره ی بیرون پنجره نگاه کردند .در حال بازگشت پای تابلو بودند که به ناگاه دیدیم خم شدند و یک مداد نصفه نیمه را با احترام از زمین بلند کردند و از بچه ها پرسیدند: این قلم مال چه کیست ؟ کسی جواب نداد . همه متحیر بودند وبا خود فکر میکردند خوب احتمالا صاحب آن مداد به دلیل آنکه دیگر اندازه ی قلمش مناسب نوشتن نبوده آن را دور انداخته است . برخی با تعجب و برخی هم با لبخندی یواشکی و معنادار به همدیگر نگاه میکردند که استاد ذکر کردند :

نون و القلم و ما یسطرون

و گفتند که خداوند متعال در قرآن کریم به قلم سوگند خورده پس هیچ گاه قلم هایتان را سبک نشمرید.

ناخودآگاه یاد مدادهای بچگی مان افتادم که هی می تراشیدیم و هی می تراشیدیم که زودترتمام بشود و یاد کاغذهایی که از وسط دفتر می کندیم که زودتردفترمان را عوض کنیم و یاد تصویری از ۱۲سال پیش شمال با آن جنگل های انبوه و زیبایش و جنگل های تنک امروز وسیل های پیاپی و...

چند روز پیش عکسی دریافت کردم که درگوشه ای از این کره ی خاکی در قسمت انتهایی مداد دانه ای قرار داده شده بود تا با کاشت مداد بی استفاده ، مجددا درختی رشد کند و باز هم مثل همیشه کلی اظهارنظر در رابطه با اینکه ما مدادهایمان را نصفه رها می کنیم وبرتری تفکر وعملکرد دیگران و....

غافل از اینکه ما در فرهنگ غنی خودمان انسانهایی داریم که

حتی با دیدن قلم روی زمین به احترام آن خم میشوند و ...

احترامی که دررفتاربزرگترهایمان بیشتر دیده می شود احترام به قلم ، احترام به نان ، احترام به گندم ، احترام به پرنده و همه اینها یعنی احترام به حیات وسپاسگزاری از خالق .

این کار استاد بزرگوارم موجب شد تا من سوره ی قلم را با دقت بخوانم در ادامه این سوره پس از سوگند به قلم وتاکید بر برتری اخلاق پیامبراعظم داستان قومی ذکر میشود که قصد برداشت محصول باغشان را داشتند وبی توجه به اراده ی الهی و بدون ذکر انشاالله به قصد دوری از چشم فقرا صبح گاهان وارد باغ شدند ؛اینجا بود که به اذن الهی باچنان باغ بی برگ وباری روبرو شدند که گمان کردند اشتباه آمده اند .

کاش می شد همه همقسم می شدیم که نگذاریم حرمت هایی که بزرگترهایمان رعایت می کردند به فراموشی سپرده شوند،که فراموشیشان موجب خسران است و ناسپاسی و قدرنشناسی نعمات الهی ...

پس بیاییم از امروز هرگاه فرد سالخورده ای را دیدیم که نان را می بوسد و از روی زمین بر می دارد پوزخند نزنیم چرا که آن فرد از حرمان نعمت جلوگیری کرده و رحمت الهی را برایمان به ارمغان می آورد . از امروز به بعد اگر کبوتری در کنج خانه مان لانه ساخت خانه اش را ویران نکنیم و مثل مادر بزرگ هایمان هوای پرنده های گرسنه و تشنه را داشته باشیم و بدانیم سهم پرنده ها چنگ ارزنی بیش نیست !!! بیاییم اگر کسی سنت های درستمان را به تمسخر گرفت با اعتقاد راسخ به برتری فرهنگمان نگذاریم داشته هایمان را با مصادره به نام خودشان به ما باز گردانند.

نویسنده: مهسا زمان

خداحافظی

امروز که برای آخرین صفحه ات مینویسم بی نهایت دلتنگم برای تمام روزهای با تو بودن برای تمام روزهایی که تو بهانه ام بودی تا فارغ از دغدغه ی همیشگی یک دانشجو لحظاتی با اساتیدم باشم و در مورد تو با انها حرف بزنیم حرفهایی که باعث پخته تر شدنت شد. امروز میخواهم بدون چارچوب حرف بزنم میخواهم تا حصارهای جملات را بشکنم و با خالصانه ترین کلمات تشکر کنم از تمام کسانی که بدون حضورشان تویی نبود میخواهم از اساتیدمان بگویم که دعوتمان را پذیرفتند و به سوالاتمان پاسخ دادند : اساتید عزیزم سرکار خانم دکتر شمس سرکار خانم دکتر طاهری و سرکار خانم دکتر اسکندری و آقای دکتر رنجبر سخنران محترم جشن هفته ی ریاضی که در آخرین مصاحبه در خدمتشان بودیم. عزیزانی که همراهیشان موجب دلگرمیمان بود و به امید دیدن لبخند رضایتشان می نوشتیم استاد طاهری عزیزم که همیشه پذیرایمان بودید هیچگاه فراموشتان نمی کنیم استاد اسکندری گرامی ممنون برای تمام اطلاعات مفیدی که در اختیارمان قرار دادید و میخواهم سپاسگزاری کنم از استادی که حتی یک بار هم موفق نشدم با ایشان درس بردارم ولی زحمت کشیدند و مقاله ی ترجمه شده مان را خواندند ایراداتمان را ذکر کردند و برایمان یک نسخه از منابع معتبرتر و واضح تر خودشان کپی گرفتند کاری که هیچ گاه فراموش نمی کنیم استاد سلطانخواه گرامی برای لطفتان سپاسگزاریم . از استاد تجویدی عزیز هم برای همراهی دوستانی که در مسابقات ریاضی سمنان شرکت کرده بودند و نیز برای راهنمایی های زمان انتخاب واحدمان متشکریم . از اساتید گرامی گروه ریاضی که قبول زحمت فرمودند و نشریه را مطالعه نمودند خانم ها دکتر اخوان دکتر هادیان و دکتر ربیعی و تمام اساتید برای تلمذ در مکتبشان سپاسگزاریم(استاد اردوخانی ، استاد بهمردی، استاد لاله ،استاد بهروزی، استاد دیوانی آذر ، استاد شاهرضایی، استاد گنجی ،استاد ملکپور استاد ملکی استاد سنجریان استاد مدبر). می خواهم از دوستان همیشه وفادارم بگویم دوستانی که حتی پس از فارغ التحصیلی با تو ماندند و برایت نوشتند از مریم عزیزم که بی او حرفهای مجله خشک و بی رونق می ماند و دستانش نگارگر صفحاتت بود . از زهرا و رویا و مهدیه جان که سه عضو دائممان بودند سپاسگزارم و آرزوی موفقیت میکنم برای دوستان جدیدمان نیلوفر و معصومه جان و سپاسگزارم از شهرزاد عزیزم که نشریه را به ما سپرد و برایش بهترین ها را آرزومندم .

اما از همه گفتیم و گفتیم و حالا نوبت پدر و مادر عزیزم میشود که بود و نبودم را مدیونشان هستم و وصفی برای عشقشان ندارم که عشق الهی را به من آموختند.

با اینکه دست تقدیر این شد که دوره ی ارشد را در کنارتان نباشم ولی همواره به یادتان هستم.

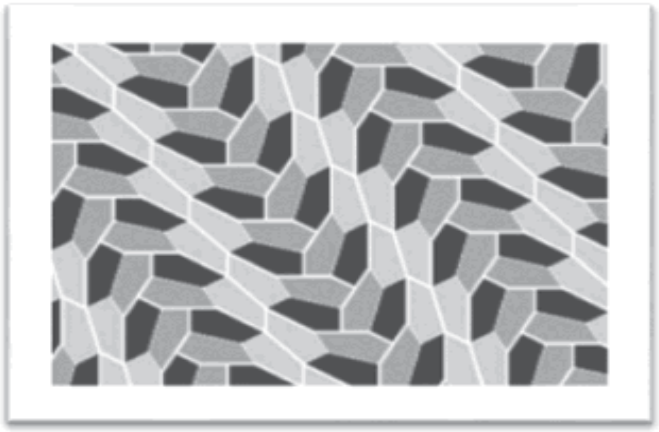
هستم اگر می روم گر نروم نیستم.. .

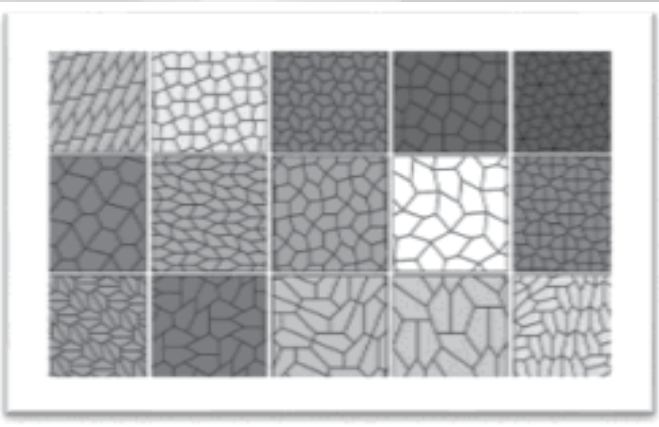
کلام آخر اینکه رادیکال دو آمد برای شکستن فضای خشک کلاس و مشق برای یافتن کاربردهای ریاضیات و کاربردها برای شما برای من تو او ما شما ایشان ....

نویسنده: مهسا زمان

نشریه علمی - دانشجویی
رادیکال ۲
پاییز و زمستان ۹۳- شماره ۱۳

با کشفی تازه ، ۳ ریاضیدان ضربه ای به یک مسئله ی حل نشده ریاضی زدند!





جنیفر مان و همسرش چسی مان به همراه همکارشان دیوید ون دراو از دانشگاه واشنگتن به وسیله ی الگوریتمی ریاضی و با استفاده از کامپیوتر یکی دیگر از جواب های مسئله ای قدیمی در ریاضیات گسسته را به دست بیاورند. این مسئله که پس از ۳۰ سال جواب دیگری برای آن پیدا شده آن است که چگونه یک صفحه را با پنج ضلعی های محدب به گونه ای پر کنیم که فضای خالی باقی نماند این مسئله قبلا برای مثلث و چهار ضلعی ها حل شده اما تعداد جواب ها برای پنج ضلعی ها نا معلوم میباشد و پیش از این تنها ۱۴ حالت ممکن در نظر گرفته میشد اما حالا بعد سال ها راه حل ۱۵ ام هم برای آن پیدا شده. جالب آنکه پیش از این دکتر مان و همکارانش که دو سال روی این مسئله کار میکردند از پیدا کردن جواب جدید قطع امید کرده بودند چون برای حل این مسئله باید احتمالات زیادی را بررسی کرد تا آنکه شکل زیر را پیدا کردند و قدمی دیگر به حل مسئله نزدیک شدند.

لینک خبر / www.npr.org

اثبات نظریه ریاضیدان در حال مرگ پس از یک قرن!

محققان دانشگاه «اموری» پس از نزدیک به یک قرن توانسته‌اند معمایی را که سرینیواسا رامانوجن، ریاضیدان هندی در بستر مرگ مدعی شده بود که در رویا به وی الهام شده، حل کنند. رامانوجن در سال ۱۹۲۰ در بستر مرگ در نامه ای به معلم خود، گادفری هارولد هاردی، ریاضیدان انگلیسی به ترسیم چندین تابع جدید ریاضی به همراه توضیحاتی در مورد شیوه عملکرد آنها پرداخت که تا آن زمان ناشناخته بود. اکنون محققان بعد از چندین دهه اعلام کرده اند که حق با این ریاضیدان بوده و اینکه این فرمول می‌تواند رفتار سیاه‌چاله‌ها را توضیح دهد. رامانوجن که یک ریاضیدان خودآموخته بود، در یک دهکده محلی در جنوب هند متولد شد .نامه این ریاضیدان محتوی چند تابع بوده که نسبت به توابع کنونی تتا یا شکلهای مدولار متفاوت هستند با این حال همچنان از آنها تقلید می‌کند. این ریاضیدان هندی حدس زده بود که شکلهای مادولار تقلیدی وی ، با شکلهای مادولار رایج که پیشتر توسط کارل جاکوبی شناسایی شده بود، مطابقت دارد و اینکه نتیجه هر دو، خروجی‌های مشابه برای ریشه‌های یک است. وی پیش از اینکه بتواند ظن خود را اثبات کند، درگذشت اما بیش از ۹۰ سال پس از مرگ وی، محققان توانستند اثبات کنند که این توابع در حقیقت از شکلهای مادولار تقلید می‌کنند اما خصوصیات توصیف‌کننده خود مانند ابرتقارن را به اشتراک نمی‌گذارند. توسعه این توابع می‌تواند به فیزیکدانان در محاسبه آنتروپی یا سطح اختلال سیاه‌چاله‌ها کمک کند. این یافته‌ها در آستانه صد و بیست و پنجمین سالگرد تولد رامانوجن در کنفرانس ۱۲۵ رامانوجن در دانشگاه فلوریدا ارائه شده است.

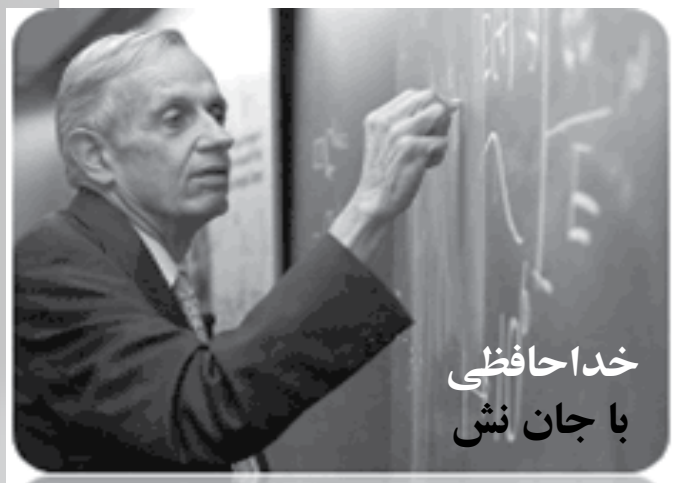
لینک خبر www.njavan.com/

در این شماره نشریه میخوام وب سایت و اپلیکیشن TED رو به شما معرفی کنم . سلسله کنفرانس های TED اولین بار در سال ۱۹۸۴ با تاکید روی پیشرفت های تکنولوژی و طراحی در کالیفرنیا برگزار شد ، اما بعد از اون در اقصی نقاط جهان گسترش یافت. در حال حاظر این کنفرانس ها در آسیا و اروپا و ایالات متحده و در موضوع های مختلف برگزار می شود و هدف از آنها پخش کردن ایده های با ارزش در سرتا سر جهای میباشد . این سخنرانی ها در موضوعات مختلف از جمله ریاضیات ، در دسته بندی های

TED
Ideas worth spreading

مدل ریاضی برای توصیف پیچیدگی دینامیک انتقال بیماری

اثر حرکت یک فرد بر روی دینامیک شیوع یک بیماری برای سال ها مورد توجه ریاضیات اپیدمیک بوده است ، به خصوص از سال ۲۰۰۲ تا ۲۰۰۳ که بیماری سارس به طور ناگهانی شیوع پیدا کرد و نشان داد که یک فرد بیمار میتواند به سرعت از طریق خطوط حمل و نقل هوایی بیماری را منتقل کند . حالا دکتر راس و همکارش مدلی ریاضی برای توصیف چگونگی تاثیر نقل مکان یک روی شیوع بیماری با رفتن از شهری به شهر دیگر ارائه داده است . دکتر راس میگوید که ابزار زیادی برای توصیف این حرکت در ریاضیات موجود میباشد از جمله مدل چند وصله ای که برای توصیف چگونگی پخش شدن یک بیماری در یک حوزه ی خاص مثلا یک روستا را توصیف میکنند. در این معادلات سعی میشود که عدد تکثیر اساسی که با R_0 نشان داده میشود و میانگین تکثیر یک بیماری را در ثانیه نشان میدهد کاهش داده شود.اگر این عدد بالای ۱ باشد بیماری به سرعت شیوع پیدا میکند اما تصور میشد که اگر این عدد زیر ۱ باشد بیماری خود به خود در چند مرحله دچار تعادل شود و بعد از مدتی دیگر تکثیر نشود اما تحقیقات جدید در ریاضیات این وضعیت نشان داد که تحت شرایطی بیماری میتواند همچنان به انتقال خود در تعداد کم ادامه دهد تا زمانی که دوباره شیوع همگانی پیدا کند . حالا دکتر راس و همکارش در مدل جدید خودشان و با کار روی این حالت مدلی ارائه دادند که ۹ وضعیت ممکن جدید را برای شیوع دوباره بیماری در حالتی که R_0 کمتر از ۱ است را پیش بینی میکند .



خداحافظی با جان نش

۲۳ می ۲۰۱۵ (۲ خرداد ماه ۱۳۹۴) جان نش (در سن ۸۷ سالگی) و همسرش آلیشیا در تصادف رانندگی جان خودشان را از دست دادند. بیشتر مردم او را به خاطر کتاب و فیلم «یک ذهن زیبا» به خاطر خواهند داشت اما جامعه ی ریاضی او را به خاطر آثار مهمش در نظریه بازی و هندسه و معادلات دیفرانسیل به خاطر خواهند داشت . او که در سال ۱۹۹۴ برنده ی جایزه نوبل در اقتصاد شده بود ، امسال هم جایزه ی آبل رو به خاطر کار در معادلات دیفرانسیل و هندسه به طور مشترک با لوئیس نورنبرگ برده بود، یادش گرامی.

لینک خبر/Plus.math.org

این سایت موجود میباشد . نکته مثبت این سخنرانی ها این است که معمولا کوتاه هستند و با حجم کم و یا حتی با فرمت MP۳ قابل دانلود هستند . نکته ی جالب تر اونکه این سخنرانی ها رو اکثراً میتوانید با زیرنویس فارسی ببینید پس اگر مشکل زبان انگلیسی دارید از این بابت هم راحت هستید .
چیزی که به شخصه برای من جالب بود اینکه دومین ویدئو پر بازدید در این سایت مربوط به خانم دکتر هانا فرای است که دکترای ریاضی دارند و عنوان سخنرانی ایشون هم «ریاضیات عشق بود» پس اگر به این وب سایت سر زدید و یا از طریق اپلیکیشن بهش دسترسی پیدا کردید پیشنهاد میکنم که این ویدئو رو حتما ببینید.
می توانید برای دریافت ویدئوی این سخنرانی به وب سایت www.ted.com مراجعه کنید و یا اپلیکیشن اون رو از گوگل پلی و یا کافه بازار دانلود کنید .

نویسنده: مهدیه ابراهیمی

گزارش روز جشن هفته ی ریاضی

نویسنده: مهسا زمان

جشن هفته ریاضی امسال نیز برگزار شد اما با یک تفاوت ویژه، چون اولین سالی بود که جشن نه در گروه که در دانشکده ریاضی برگزار می شد ؛ دانشکده ی جدید التاسیسی که در همین ابتدای دانشکده شدن تفاوتش با گروه کاملا مشهود بود ؛ به همین بهانه از ریاست محترم دانشکده کمال تشکر را داریم.

ابتدای مراسم مزین شد به تلاوت آیاتی چند از کلام ا.. مجید سپس ریاست محترم دانشکده سرکار خانم دکتر شمس ، دانشکده ی ریاضی و چشم انداز پیش روی آن را معرفی کردند . در ادامه سرکار خانم دکتر گویا استاد آموزش ریاضی دانشگاه شهید بهشتی به ایراد سخنانی در مورد ریاضیات ایرانی اسلامی پرداختند . ایشان اذعان داشتند که :

«ریاضی ایرانی اسلامی سه وجه برجسته دارد که آن را از ریاضیات یونانی جدا میکند:

۱- ریاضیاتی به شدت کاربردی ؛ که ریشه در نیازهای واقعی اجتماعی دارد و مسائل روز را حل میکند مسائلی که راههای آینده را باز میکند و تنها با مسائل انتزاعی ذهنی کار نمیکند ؛ خیام نمایندهی بارز این نگاه است.

۲-ریاضیاتی محاسباتی ؛ که اکنون در دورهی جدید با توسعهی تکنولوژی و انواع نظامهای هوشمند توجه ویژه ای به آن میشود. ریاضیاتی که ایران به جهان عرضه کرده شامل: مثلثات، جبر، جبرمحاسباتی(دارای انواع الگوریتمها و محاسبات است) انواع معادلات و حل آنها ؛ انواع هندسه ها که برخلاف هندسه یونانی با واقعیت ها ، شهود و ملموسات گره خورده میباشد.

۳-ریاضیات ایرانی اسلامی ؛ که بین ریاضیات محض و کاربردی خط کشی نمیکرده.

هم چنین ایشان نقدی به پذیرش بالای دانشجو در رشته ی ریاضی داشتند و گلایه کردند : عمومی کردن ریاضی بدین معنا نیست که در هر کوی و برزن به هر کسی مدرک کارشناسی و کارشناسی ارشد داده شود عمومی سازی یعنی از تمام ظرفیتهای بالقوه و قابلیتها ریاضی استفاده کنیم تا شهروندان بهتری تربیت کنیم. شهروندانی که انتخابهای بهتری داشته باشند .

به عقیده ی ایشان ظرفیت پذیرش بالای دانشجو در رشته ی ریاضی نه تنها باعث افت کیفیت آموزشی می شود بلکه برخی دانشجویان بدون علاقه و صرفا به خاطر ورود به دانشگاه این رشته را انتخاب می کنند؛ البته آموزش ریاضی از حقوق شهروندی است و نظام آموزشی وظیفه دارد ریاضیاتی را که پایههای فکر کردن، منتقد بودن، مشاهده گری خوب، دقت در اصول، توانایی تقریب و تخمین زدن و ازهمه مهمتر توانایی حل مسائل واقعی وطرح مسئله را دارا میباشد، ارائه دهد. ریاضی میبایست مردمی باشد نه عمومی تا بتواند فاصله موجود میان عاج نشینان یونانی و دیگران را از بین برد. از طریق ریاضیات افراد امتیاز بهتر زیستن را بدست میآورند ؛امتیازی که حق همه میباشد و باید به همه داده شود و نباید تنها در انحصار عدهی خاصی باشد تا افراد بتوانند در این دنیای پرغوغا و پر انتخاب، انتخابگران بهتری باشند و این تنها با توانایی استدلال کردن حاصل میشود.

پس از خانم دکتر گویا نوبت به ارائه ی دستاوردهای آقای دکتر رنجبر متخصص جراحی قلب رسید که در این شماره مصاحبه ای خواندنی و جالب با ایشان داشته ایم، برای درک صحبت های ایشان لازم بود دانشجویان با مفاهیم پایه ای بیولوژیکی آشنایی داشته باشند به همین جهت ایشان در ابتدا به شرح الگوی پمپاژ قلب و نحوه ی حرکت خون در شریان ها پرداختند سپس به توضیح در مورد نحوه ی استفاده از نرم افزار متلب در آنالیز داده ها پرداختند . مطلب جالب توجه این بود که ایشان قبل از انجام جراحی های باز که مشقات فراوانی را برای بیمار به همراه دارد، با استفاده از روش های کاردیوگرافی به تشخیص دقیق

محل بیماری می رسند که باعث میشود آسیب کمتری به بافت طبیعی بدن بیمار برسد. ما در این شماره سعی کرده ایم در مصاحبه ی اختصاصی با ایشان شما را با موضوع اختراعشان آشنا کنیم هر چند که به دلیل گستردگی موضوع ، مانند این است که قطره ای از دریا برایتان به ارمغان آورده باشیم.

خلاصهای از سخنان جناب آقای دکتر سعید رنجبربا موضوع مدل سازی ریاضی بطن چپ و کاربردهای آن در علم کاردیولوژی را در ذیل مطالعه میکنید:

«در این تحقیقات به مطالعه شکل بافتهای عضلانی قلب پرداختیم، وشواهدی را بر اینکه این بافتها به شکل مار پیچ حلزونی Herical هستند چه در حالت سکون و چه در حالت حرکت به دست دادیم. و با استفاده از مدل سه بعدی تاری قلب در دینامیک سیالات (در این جا منظور از سیال خون است) این امکان فراهم شد که مدلی از حرکت خون در بطنها بدست آید. و توسط نرمافزار دینامیک قابل نمایش در کامپیوتر باشد. به طور عکس هم با مشاهده تغییر حرکت خون در بطن میتوان انواع پاتولوژیهای قلبی را تشخیص داد. مدلی سه بعدی از حرکت میوفیبرلهای بطن چپ دادیم، که مهمترین دستاورد در تشخیص انواع پاتولوژیهای قلبی است و همودینامیک خون و در ساخت قلب مصنوعی.موارد کاربرد بالینی این مطالعه:

۱-با ساخت نرمافزاری که قابل نصب در دستگاه اکو باشد پزشک میتواند حرکت تارهای عضلانی را بطور میکروسکوپی مشاهده کند. به این ترتیب با تغییری که در حرکت فیبرهای عضلانی قلب در پاتولوژی-های مختلف به وجود میآید، میتوان به راحتی نوع پاتولوژی را تشخیص داد.و نیاز به تجربه بالا در اکو کاردیوگرافی را حذف نموده و شرایط پاتولوژیک را به سهولت و در بالین بیمار تشخیص داد.

۲-کاربرد این مطالعه در ساخت قلب مصنوعی: دستگاههای قلب مصنوعی فعلی، عملا فقط نقش یک پمپ را دارند که این سبب افزایش tubulance جریان خون و مرگ گلبول قرمز میشود. زیرا حرکت قلب طبیعی را ندارد. اما با پیاده کردن این الگوریتم حرکتی روی پلیمر و ساخت قلبی که این منحنی حرکت در آن لحاظ شده باشد، به ساختار قلب نزدیکتر شده و کارکرد طولانی تری میتواند داشته باشد.

۳-با مطرح شدن جراحی رباتیک دربعضی اعمال جراحی و داشتن نرم افزار حرکت تارهای عضلانی عملا این امکان فراهم می-شود که به صورت هوشمند ربات محلهای پاتولوژیک را شناسایی و روی آن حرکت نماید.

۴-در بسیاری از کاربردها ما با یک سیال غیر تیوتونی با ویسکاسیته بالا سروکار داریم که رفتار جریان در آنها متفاوت باسیالات عادی است و مدلسازی و تحلیل مختص خود را می-طلبد. یکی از مثالهای مهم این سیالات، خون در شریانهای بدن انسان است که از جهت اختلالات قلبی عروقی بسیار مورد توجه و حیاتی میباشد. از این رو ارائه یک مدل ریاضی مناسب برای جریان سیال غیر تیوتونی در تیوبی فشرده و تحلیل ریاضی آن، ما را در شناخت هرچه بهتر کاری شریان و وریدها کمک فراوانی میکند. الاستیک بودن عروق در کنار جریان سیال پیچیدهای مانند خون و ارتباط آنها با یکدیگر این مسئله را از نظر ریاضی بسیار مشکل میکند.

انتخاب یک مدل مناسب که پاسخگوی مسائل مطرح در اختلالات قلبی و عروقی باشد هدف اصلی است؛ سپس به تحلیل ریاضی این مدل میپردازیم و بر اساس این تحلیل ریاضی روش-های عددی کارآمدی را برای تحلیل عددی این مدل انتخاب میکنیم ؛ سپس با استفاده از دستاوردهای تحلیلی عددی میکوشیم راهکارهایی برای مثال در راستای عمل جراحی مجازی ارئه دهیم.

پس از سخنرانی آقای دکتر رنجبر، خانم دکتر رقیه زارعی از گروه زیست شناسی مطالبی در مورد ارتباط اعداد و نسبت های موجود در طبیعت بیان نمودند و فیلم جالبی که با همین مضمون تهیه نموده بودند ، در خلال سخنرانیشان به اجرا درآمد.

سپس خانم دکتر فاطمه آهنگری، عضو جدید هیئت علمی دانشگاه الزهرا به بررسی رویکرد کلی کاربرد هندسه در سایر شاخههای علم و فناوری پرداختند؛ و کاربرد هندسه را در سه حوزه مهم بکارگیری هندسه در صنعت هوا و فضا، بکارگیری هندسه در فناوری نانو و بکارگیری هندسه در کیهان شناسی تبیین نمودند. ایشان با تحلیل جریان های هوایی هنگام حرکت هواپیما و جریان های ناگهانی باد تلاش کردند تا الگویی از حرکت هواپیما در طوفان را ارائه دهند. این کار موضوع پروژه ی دکترای ایشان بود که با جذابیت های خاص خودش همراه بود.

پس از اجرای سخنرانی ها سرکار خانم دکتر طاهری مدیرگروه محترم ریاضی شعر زیبایی را قرائت نمودند. استاد طاهری، استاد راهنمای انجمن ریاضی در دانشگاه الزهرا هستند که به واسطه ی فعالیتشان در انجمن، بچه های نشریه و انجمن علمی همیشه از راهنمایی های ایشان استفاده می کنند و حقیقتا در فعالیت های انجمن ریاضی بدون کمک گرفتن از ایشان ادامه کار دشوار است.

در خاتمه دانش آموختگان تجربیات تحصیلی شان را بازگو کردند و خانم فاطمه ربیعی از خاطراتشان در المپیاد گفتند ودانشجویان را برای شرکت در مسابقات سال های آینده ترغیب کردند. ایشان تنها با مرور دقیق جزوات تحقیق در عملیات استاد تجویدی قادر به پاسخگویی به ۴ سوال از ۱۲سوال بودند. البته دلیل اینکه فقط در مورد جزوه ی استاد تجویدی گفتیم این بود که به گفته ی خانم ربیعی ایشان در مدت زمان کوتاهی که به المپیاد مانده بود فقط به مطالعه درس تحقیق در عملیات پرداختند.

و در پایان نیز بنده به نمایندگی از بچه های نشریه ی رادیکال ۲ از زحمات اساتید گرامی در طول دوره ی تحصیلی مان قدردانی نمودم.

جشن امسال فرصتی بود کوتاه برای دیدن فعالیت های بین رشته ای صورت گرفته توسط محققان کشورمان ؛ فرصتی که بایستی غنیمت شمرده میشد تا آنچه نادیدنی است را میدید ؛ فرصتی برای رسیدن به پاسخ این سوال: استاد حالا این درسی که خوندیم به چه دردمون میخوره... !!!

تحلیل ریاضی نوای قلب

سعید رنجبر مدرک دکتری ریاضی خود را در سال ۲۰۰۸ و در گرایش هندسه جبری از دانشگاه تربیست اخذ نموده و در سال ۲۰۱۳ موفق به دریافت مدرک تخصص جراحی قلب از دانشگاه ایلینوی شیکاگو شده است وی هچنین عضو تیم تحقیقاتی اکوکاردیو گرافی شرکت ازاوته است و نرم افزار (Imaging Cardiolog) را اختروع و در آمریکا به ثبت رسانده است.

برای اولین سوال که فکر می کنم تقریبا سوال تمام مخاطبان نشریه باشه ، دوست دارم راجع به این نقطه ی عطف برامون بگید که چی شد تصمیم گرفتید از ریاضی به پزشکی تغییر رشته بدید؟

در سال دوم دبیرستان بودم که با کتاب «دیدگاه های نوین ریاضیات در پزشکی» آشنا شدم و با شوق فراوان به سرعت و دقت بالا آن را تا به آخر مطالعه کردم. در آن کتاب بیشتر به عملکرد مغز با زبان گراف ها در ریاضیات پرداخته بود بدین صورت که گرافی را معرفی میکرد که راس هایش نرون ها و یال هایش سیناپس ها بودند که نرون ها را به هم وصل می کردند. و بدین ترتیب بود که الگویی ساده از رفتار های عصبی را با تحلیل گراف مربوطه اش ارائه می دادند. بسیاری از بیمارهای روانشناختی را بدین روش با تکنیک ها و ابزار های ساده ریاضیات مدل سازی می کردند. مطلب مهم ایده ها و تفکرات هوشمندانه و زیرکانه ریاضی هستند که حائز اهمیتند و البته بی ارتباط با ایده های کلی در شاخه پزشکی مربوطه نمی توانند باشند. . در آن زمان من با برخی از جنبه های کاری ریاضیدانان معروف از جمله نیوتن و کارل فردریش گائوس آشنا بودم. می دیدم که این افراد در زمینه های دیگر علوم نیز خلاق و مبدع بودند مثلا کارهای گائوس در مغناطیس به همراه وبر و کارهای نیوتن در فیزیک و نور بسیار قابل توجه در درک فهم تئوری های محض شان نیز می شدند. این شد تصمیم گرفتم ابتدا وارد رشته ریاضیات که پایه تمامی علوم بود را ادامه دهم.

البته در آن دوران طراحی ساختار ریاضی و عملکرد قلب در ذهنم بود. پس از اتمام دکترا در هندسه جبری و آشنایی با حل و آنالیز تحلیلی و عددی جواب های معادلات دیفرانسیل با مشتقات جزیی بود که تصمیم به تحقق بخشیدن به افکاری که از زمان دبیرستان در سر می پروراندم، گرفتم و آن هم مدل سازی ریاضی قلب بود به طور اخص سمت چپ قلب. بدین منظور وارد شاخه کاردیولوژی شدم و فلوشیپی اکوکاردیوگرافی را از انجمن آکادمیک اکوکاردیوگرافی آمریکا گرفتم زیرا که کار بروی ارگانی مانند قلب بدون شناخت قلب، آن هم شناختی با تمام جزییاتش برای انجام کاری جدی غیرممکن بود.

برای کسانی که در جشن هفته ی ریاضی حضور نداشتند کمی از اختراعتون بفرمایید.

اختراعاتم مربوط به طراحی و ساخت ۳ نرم افزار ریاضی در مدل سازی بطن چپ، مسیرهای حرکتی خون داخل بطن چپ و گرمای مبادله شده بین خون و عضله بطن چپ قلب بودند که نرم افزار سومی راه حلی برای تعیین میزان تنگی عروق قلبی با روشی جدید و ریاضی طراحی و ساخته شده است که امیدواریم در آینده بیماران بدون نیاز به آنژیوگرافی میزان دقیق گرفتگی عروقشان مشخص شود.

چون مدل شما نمونه ی موفق و عملی یک پژوهش هدفمند است در مورد نحوه ی جمع آوری داده ها و موانعی که برای گردآوری داده های صحیح پیشرو داشتید بفرمایید و اینکه در روند این اختراع جایی بود که به درستی داده ها شک کنید یا در حل مساله به تناقض و ناهمگونی برسید؟

داده های من مقالات ، کتاب ها، یادگیری شاخه دوم (کاردیولوژی) و آشنایی با سیستم های تصویر برداری قلبی عروقی از جمله دستگاههای اکوکاردیوگرافی و ام ار آی قلبی، نحوه تشخیص بیماری های قلبی با این دستگاه ها و به طور بالینی همزمان، مشاهدات، حضور در ده ها هزار عمل های جراحی قلب، یافتن پل های ارتباطی این دانسته ها با ریاضیات و مهم تر از همه شاگردی و همصحبتی با افراد و اساتید مختلف بودند که روند چگونه اندیشیدن به مساله و شناختن موانع سر راه را روشن میکردند. اگر بخواهم مکاتبات و مذاکراتم را که با صدها استادهای به نام در سراسر دنیا اعم از دانشگاه ها مراکز علمی و دانشمندان بخش سیستم های تصویربرداری قلبی کمپانی هایی مثل فیلیپس ، توشیبا، جنرال الکتریک و زیمنس داشتم ، بنویسم خود کتابی می شود که روزی انشاله این کار را خواهم کرد. داده های بیماران مدام با این سیستم های تصویر برداری گرفته میشدند و بارها و بارها تحلیل و با سیستم ها و متد های مختلف و شواهد و تجربیات و تعبیرهای واقعی چک می شدند و مدام بازسازی و بازنگری می شدند که مدل سازی ها با آنچه هست مطابقت داشته باشند. گاه مدلی درستیش و میزان دقتش بعد از عمل های جراحی بررسی می شد و موانع را نشان میداد و راه حل رفع آن نیز مشخص می شد.

من در چکیده ی یکی از مقالات شما خواندم که شما فقط با ۷۰ نفر که به طور داوطلبانه با شما همکاری کردند موفق شدید تا مقیاس های مورد نیاز در پروژه را روی قلب سالم اندازه گیری کنید ، فکر میکنم برای همه جالب باشه که چطور فقط با استفاده از داده های ۷۰ نفر بتوان برای همه تصمیم گیری کرد و اینکه چه ویژگی هایی از نظر سن و جنس و اندازه قلب در آن ۷۰ نفر بوده که قابل تعمیم به همه ی آدم ها شدند؟

تکنیک های ریاضی و ایده ها ی خلاقانه نقش اصلی را داشتند که اکثرا از روی مشاهدات، مطالعات و تفکر بسیار ساخته و بازسازی و گسترش داده می شدند. . توابع و فرمول های به دست آمده متغیر های زیادی را داشتند از جمله سن و جنس و اندازه و حرکت قلب افراد و ... به عبارتی دیگر نرم افزار ما با توجه به هر مریض یک مدلینگ از بطن چپش میدهد. خوبی مدلینگ ما این هست که از فرضیات کلی برحذر بوده و نرم افزار ساخته شده کاملا وابسته به اطلاعات بیمار مورد نظر است و مدل قلب وی را بازسازی در جهت امر تشخیص و درمان می کند. ۷۰ نفر به عنوان مثال بررسی شدند. با این نرم افزار هرکس مدل حرکتی و ساختار تاری قلبش را به دقت می تواند ببیند.

چه قابلیت هایی در نرم افزار متلب دیدید که آن را برای مدل سازی استفاده کردید؟

نرم افزار MATLAB نرم افزاری بسیار توانمند هست چه در بررسی و حل عددی معادلات دیفرانسیلی که حل شان با روش های پیشرفته تحلیلی انجام می شدند و مقایسه های نمودارهای حل جواب ها با یافته های کلینیکالی و مطابقت با آنها. و نیز کدسازی الگوریتم های ریاضی طراحی شده. و تکنیک های ریاضی پردازش تصاویر و یافتن داده های عددی پنهان از تصاویر مانند کدگشایی. و ....

مطابق گفته های شما به نظر میرسد که اگر اقدام به موقع برای فردی صورت بگیرد، که احتمال وقوع سکته و نارسایی به حداقل می رسد. نظرتان در این شرایط چند سال به عمر مفید بیماران اضافه می شود؟ آیا قابل پیش بینی است؟

بله قابل پیشبینی است. لازم به ذکر است تقریبا اکثر بیماران از بیماری شان نیست که میمیرند بلکه از نحوه درمان شان هست که میمیرند. تشخیص به موقع و نحوه درمان درست، بیمار را نه تنها نجات می دهد بلکه این از خواص بدن ما است که خودش را به حالت نرمال می رساند و عمر طولانی تری میابیم.

آیا به دلیل وجود گره سینوسی-دهلیزی بود که فقط روی بطن چپ کار کردید یا امکان مدل سازی دهلیزها هم وجود دارد؟

خیر. به دلایل زیادی که از اهم آنها به نقش اساسی عملکرد بطن چپ در قلب میتوان اشاره کرد.

بله امکان مدل سازی دهلیز ها هم وجود دارد اما توضیحش در این مجال نمیگنجد.

نرم افزار Solution Navier-stocks equations of the blood as a non-Newtonian fluid in the left ventricle در سازمان ثبت اختراعات و علائم تجاری آمریکا (USPTO) در ژانویه ۲۰۱۴ مورد پذیرش قرار گرفت و مجوز صدور ثبت (Notice of allowance) را کسب کرد این اختراع در مجامع بین المللی مختلفی به صورت سخنرانی و پوستر ارائه شد.

نرم افزار System and Method for modeling left ventricle of heart به مطالعه شکل بافت‌های عضلانی بطن چپ قلب می‌پردازد و مدل تاری سه بعدی از بطن چپ ارایه می‌دهد. با استفاده از این مدل سه بعدی تاری بطن چپ در دینامیک سیالات(خون) این امکان فراهم شد که توسط نرم افزار Solution Navier-stocks equations of the blood as a non-Newtonian fluid in the left ventricle مدلی از حرکت خون در بطن چپ بدست آید و توسط آن قابل نمایش در کامپیوتر باشد و به طور برعکس هم با مشاهده تغییر حرکت خون در بطن می‌توان انواع پاتولوژی‌های قلبی را تشخیص داد.

با ساخت (software) نرم افزار که قابل نصب در دستگاه اکو باشد پزشک می‌تواند حرکت تارهای عضلانی را بطور دقیق تری بررسی کند. به این ترتیب با تغییری که در حرکت فیبرهای عضلانی قلب در پاتولوژی‌های مختلف بوجود می‌آید، می‌توان به راحتی نوع پاتولوژی را تشخیص داد.

ایشان با اشاره به اینکه نرم افزار مذکور در ساخت سیستم‌های قلب مصنوعی استفاده می‌شود تاکید کرد: دستگاههای قلب مصنوعی فعلی عملاً فقط نقش یک پمپ را دارند و این امر سبب افزایش turbulance جریان خون و مرگ گلبول قرمز می‌شود؛ زیرا حرکت یک قلب طبیعی را ندارد اما با پیاده کردن این الگوریتم حرکتی روی پلیمر و ساخت قلبی که این منحنی حرکت در آن لحاظ شده باشد، به ساختار قلب طبیعی نزدیکتر بوده و کارکرد طولانی‌تری می‌تواند داشته باشد.

با فرض اینکه برای دهلیزها هم مدل سازی داشته باشیم آیا می تواند به این معنا باشد که با اقدام به موقع امکان حیات مجدد برای بیماران فراهم می شود؟

بله در بالا کمی توضیح دادم. نه تنها می توان به بیماران حیات دوباره داد بلکه می توان از بیماری های مادرزادی زمانی که جنین در شکم مادر هست پیشگیری کرد. جالب بدانید ریاضیات قلب جنین بسیار شگفت انگیز و پیچیده است. و دانستن چگونه ساخته شدن بطن ها و دهلیز ها و دریچه ها خود بازگو کننده خواهد بود که چطور از بیماری های مادرزادی نوزادانمان جلوگیری کنیم مثلا دچار سوراخ بین بطنی یا دهلیزی نشوند که اتفاقا این امر اگر اتفاق بیافتد در روزهای ۲۲-ام تا ۳۰-ام که جنین داخل شکم مادر هست اتفاق خواهد افتاد و مادران باید نکات بسیاری را در این بازه زمانی رعایت کنند.

آیا تا کنون به موردی برخورد کرده اید که به کمک روش ابداعی شما امری محال به ممکن تبدیل شده باشد؟

بله زیاد. در امر تشخیص بیماری هایی که دیگر تجربه موثر نیستند و ارائه و پیشنهاد برای درمان. مثال های زیادی هستند که در این مصاحبه به علت تخصصی بودن مطالب به ذکر انها نمی پردازم.

به نظر شما کاربردی ترین حوزه ی ریاضی بعد از پزشکی چیست؟

مکانیک آسمانی، نجوم ، کیهان شناسی که به تازگی ریاضی دانان بسیاری را متوجه خودش کرده و کاربردهایی باورنکردنی حتی در رشد زندگی بشریت دارند.

خیلی ها تصور میکنند که علوم محض بی ارتباط به پدیده های جهان هستی است ولی عملا اینگونه نیست نظرتان راجع به مرزبندی ریاضیات به کاربردی و محض چیست؟

هیچ مرزی وجود ندارد.

چه توصیه ای برای یافتن زمینه های کاربرد ریاضی در حل مسائل دارید(برای دانشجویان علاقه مند به حل مسئله)؟

کار زیاد، تفکر و همنشینی با اساتید و دانشمندان و ادم های خلاق در سایر علوم.

ممنونم که قبول زحمت فرمودید و در مصاحبه شرکت کردید.

گزارشگر: مهسا زمان

اولین MISSION بنیاد نیک ورزی شریان

● زمان : ۱۰ الی ۲۳ مردادماه ۱۳۹۴

● مکان : بیمارستان مرکزطبی تهران

انجام عمل جراحی قلب جهت ۳۶ کودک محروم کشور با بیماری شدید مادرزادی قلبی با همکاری تیم جراحی قلب نویک، یک تیم فوق تخصصی از کشورهای آمریکا و کانادا و قاره اروپا تحت عنوان جهت همزمانی انجام عمل خیرخواهانه و انتقال دانش نوین جراحی قلب اطفال به متخصصین کشور عزیزمان ایران

بنیاد نیک ورزی شریان

ما (هیات موسس) با نیت تسکین آلام و اندوه پدران و مادران سرزمین عزیزمان ، برای هدیه کردن نعمت سلامت جسم و جان کودکان عزیزی که آینده سازان این مرز و بوم خواهند بود به میدان آمده ایم و توان اندیشه - برنامه ریزی و اجرایی خود را در طبق اخلاص نهاده و به امید کمک های فکری - اجتماعی - اجرایی و اقتصادی نیک اندیشان و خیرخواهان این مرز و بوم راهی را آغاز کرده ایم که به ادامه خیر و مسیر رو به تعالی آن ایمان داریم .

از این رو به انتظار دریافت رهنمودها و کمک های توانمندان اجتماع به نجوای عشق و دوستی با شما آمده ایم تا همدل و همزبان همراه شویم و دستی از دوستی و یاری به سوی دستهایی که برای دریافت حمایتی دراز شده اند بگشائیم. و با استعانت از ذات متعالی پروردگار و طینت الهی بشر گامی را برداریم که شایسته مخلوقی است که از روح پروردگار در او دمیده شده است

شماره حساب بانک سامان

۸۸۲۸۱۰۸۸۲۸۱۰۱۱

شماره کارت

۶۲۱۹۸۶۱۰۲۰۹۲۵۵۳۲

بنام : بنیاد نیک ورزی شریان

کودکان نجات یافته امروز سازندگان خلاق فردایند

اهداف

توسعه فرهنگ انفاق از طریق به اشتراک گذاشتن زمان و تخصص توسط افراد متخصص و مرتبط به علوم پزشکی و غیرپزشکی جهت ارائه خدمات تخصصی به افراد نیازمند در حوزه قلب و نوزادان و کودکان.

ایجاد زیرساخت های لازم و متکی به جدیدترین دانش روز و امکانات مورد نیاز و اجرای انواع روش های درمانی-جراحی-مراقبتی-محافظتی-تکمیلی-بریج و غیره قلب نوزادان و کودکان تا سن هجده سالگی.

ایجاد سایت و بانک اطلاعاتی از آخرین دست آوردها در حوزه فعالیت های بنیاد به منظور ارتقاء آگاهی و دانش افراد جامعه.

تلاش در جهت جذب نخبگان،خبرگان و اساتید در حوزه قلب و عروق اطفال از سرتاسر دنیا جهت درمان بیماریهای صعب العلاج گروهه هدف و آموزش همزمان گروه های مختلف درمانی ایرانی توسط آن نخبگان.

فراهم آوردن زیرساخت های لازم و امکانات و اجرای روش های حمایتی حیاتی برون پیکری خاصه روش هایی مانند اکسیزناسیون غشایی برون پیکری قلب مصنوعی تجهیزات کمک قلبی-تنفسی مانند LAVD,RVAD و دیگر تجهیزاتی که در آینده ساخته خواهند شد جهت نوزادان نارس و نوزادان با بیماریهای قلبی تنفسی ریوی و کودکان با اینگونه بیماری های مادرزادی یا اکتسابی به طوری که حیات آن ها با بالاترین کیفیت ممکنه ادامه یابد و به کمک این روش های فوق الذکر بعد از عمل جراحی یا حتی بدون عمل جراحی به بهبودی کامل برسند و یا جهت درمان های تکمیلی دیگر مانند پیوند قلب، ریه و بقیه ارگان های حیاتی زمان کافی فراهم گردد.

بنیاد نیک ورزی شریان

A CREATIVE ADULT IS A CHILD WHO'S SURVIV

A CREATIVE ADULT IS A CHILD

دلنوشته های قطره
۹۳/۲/۲-(۱)

«آئینه»

گاهی که در آینه نگاه می کنم یک موجود
خرفت، زشت، کریه و گناهکار می بینم، مورد
غضب خدا و مورد لعن خلق خدا و فکر می کنم چطور می
شود چنین آدم زشتی را دوست داشت؟
چرا گفته اند باید خودتان را دوست داشته باشید تا بتوانید دیگران را
هم دوست داشته باشید؟
یک وقتها وقتی در آینه نگاه می کنم از زیبایی خود در شگفت می شوم!! و به
زبانم می آید»تبارک اله احسن الخالقین»، شنیده بودم که هر وقت در آینه نگاه
می کنید چنین بگوئید.
حتی مدتی است هر وقت یک آدم خوشگل یا یک بچه را می بینم، همین جمله را
می گویم.
بعد یک روز فکر کردم چرا اینقدر تفاوت در نگاه است؟ من که همانم، ولی یک روز
خود را در آینه زشت و پلید و سیاه می بینم و روزی دیگر زیبا و پاک وسفید! گاهی حتی
از زیبایی خلقت بند بند انگشتانم در تعجب می مانم. به تعبیری محو جمال خود می شوم،
محو زیبایی خلقت خدا، چگونه همه چیز را به ضرورت و به جا آفریده و کم وکسری
جایی باقی نگذاشته؟
فکر کنم این خاصیت آینه است که هر آنچه در وجود ماست نشان می دهد ومنعکس
می سازد، اما نه فقط آنچه در جسم و ظاهر ماست بلکه آینه افکار و ذهنیات و
احساسات ما را به خودمان نشان می دهد. روزی که فکر خوب و زیبایی داریم و شاکر
و سپاسگزارخداوندیم خودمان و همه دنیا را خوب می بینیم و آن چیزی که آینه
منعکس می کند چیزی جز نگاه خوب ما به خود و دنیای مان نیست. روزی که
بد فکر می کنیم و ناسپاس و ناراضی از خود و دنیا هستیم آینه هم همان را
منعکس می کند.
یاد آن شعر افتادم که: ... خود شکن آئینه شکستن خطاست.
شما چه فکر می کنید؟

گاهی در میان این شلوغی زندگی، گاهی درنگ
کن.
در آینه چه می بینی؟

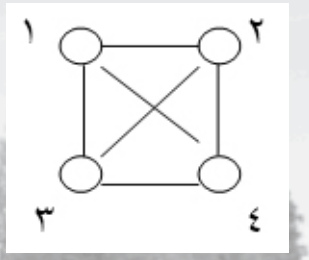
نویسنده: قطره

برنامه ریزی ورزشی :مشکلات و راه حل ها

نویسنده: زهرا جوادی

ورزش به یک تجارت جهانی مبدل شده است.بازی ها توسط میلیون ها تماشگر در سراسر جهان دنبال میشوند .تیم ها سرمایه گذاری های کلانی روی بازیکنان جدید میکنند.شهرها و کشورها بر سر میزبانی بازی هایی همچون المپیک و جام جهانی فوتبال جدال دارند.
لیگ های حرفه ای ورزشی با میلیون ها تماشگر ،سرمایه گذاری های کلان بر روی بازیکنان ،حق پخش ها،تبلیغات و مسائل مربوط به حداقل رساندن مشکلات سر و کار دارند.در مقابل لیگ های غیر حرفه ای با حجم کمتری از سرمایه گذاری سر و کار دارند ولی همچنان نیاز به هماهنگ کردن تعداد زیادی تورنومنت و بازی ها دارند.

مشکلات اصلی برنامه ریزی ورزشی شامل تعیین محل و زمان برگزاری هر کدام از بازی ها در یک تورنومنت است.برنامه ریزی عدد صحیح ،برنامه ریزی محدودیت ها ،برنامه ریزی اکتشلفی و روش های هیبرید توانسه اند راه حل هایی با متغیرهای گوناگون ارائه دهند.برنامه های کاربردی در رابطه با برنامه ریزی بازی های بسکتبال،بیسبال،فوتبال ،کریکت و هاکی یافت شده اند.در برنامه ریزی های مربوط به بازی های ورزشی برای ارائه بهترین نوع برنامه ریزی جنبه هاب متفاوتی را باید مد نظر گرفت.در برخی از آنها باید محدودیت مینیمم کردن فاصله ی طی شده را به صورت ویژه مد نظر گرفت که در بازی های رفت و برگشت در بیشتر کشورهای جنوب آمریکا رایج است.در برخی دیگر از مسائل هدف ،کم کردن تعداد breakهاست که به معنی جفت تعداد بازی های خانگی پشت سرهم یا جفت بازی های خارجی پشت سرهمی است که توسط یک تیم بازی میشود.
تورنومنت ها را میتوان با گراف نمایش داد .که هرکدام از بازی ها را یک یال نمایش میدهدو هرکدام از راس ها بیانگر یک تیم است.



به طور مثال تابه هدف minکردن مسافت پیموده شده توسط هرتیم:

$$\min F_1(z,y) = \sum_{t=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n} d_{ij}.y_{tij}$$

d_{ij} :مسافت طی شده است از شهر تیم iاست به شهر تیم j

y_{tij} :مقادیر صفر و یک را اختیار میکند،یک در شرایطی که تیم t ازموقعیت تیم iبه موقعیت تیم j سفر کند و صفر در غیر از این حال

تعدادی از محدودیت های آن نیز به شرح زیر است

$$\sum_{q=1}^{n-1} z_{tjq} = 1 \qquad \sum_{q=1}^{n-1} z_{tjq} = 0$$

۱-هر بازی در مجموعه بازی های پیش بینی شده فقط یک بار صور

$$\sum_{\substack{i=1 \\ i\neq t}}^{n} \left(z_{tjk} + z_{jtq}\right) = 1$$

۲-هر تیم در هر دور یک بار بازی میکند.

و بسیاری محدودیت دیگر که هرکدام به شکلی =کار آمد در مساله قرارمیگیرند.

باید در نظر گرفت که تعداد کمی از برنامه های نوشته شده با تکنیک های برنامه نویسی عدد صحیح و غیره در زمان بندی بازی ها به شکل عملی استفتده شده اند.
اما میتوان به نمونه هایی همچون الگوریتم شاخه و کران برای لیگ استرالیاو آلمان،برنامه نویسی عدد صحیح برای لیگ ایتالیا اشاره کرد.

منبع:sport scheduling: Problems and applications by :Celso c.Ribeiro

نویسنده: مریم بهاری

حل تقریبی معادلات انتگرال آبل

مقدمه (کلیت کار) :
در این مقاله سعی شده یک روش جدید و پایدار و تقریبی برای حل معادله انتگرال آبل ارایه شود. برای این کار بسط تیلور تابع مجهول را می نویسیم و در خود معادله انتگرال آبل جایگذاری می کنیم. به این صورت معادله انتگرال آبل تبدیل می شود به سیستمی اط معادلات خطی برحسب تابع مجهول و مشتقاتش.
حال این دستگاه را به صورت ماتریس نوشته و با استفاده از قواعد کرامر حل اش می کنیم و تابع مجهول بدست می آید.

شکل استاندارد معادله انتگرال آبل به صورت زیر است:

$$1.\ \int_0^s \frac{\emptyset(t)}{(s-t)^v}dt = f(s) \quad s>0 \qquad 0<v<1$$

$$2.\ \int_s^a \frac{\emptyset(t)}{(t-s)^v}dt = f(s) \quad s<a \quad 0<v<1$$

ما می توانیم با استفاده از تبدیلات لاپلاس برای معادلات انتگرال ۱و۲ جواب دقیق به صورت زیر بدست آوریم:

$$1.\ \emptyset(s) = \frac{\sin(v\pi)}{\pi}\frac{d}{ds}\int_0^s \frac{f(t)}{(s-t)^{1-v}}dt$$

$$2.\ \emptyset(s) = \frac{\sin(v\pi)}{\pi}\frac{d}{ds}\int_s^a \frac{f(t)}{(t-s)^{1-v}}dt$$

ما می خواهیم روشی تقریبی ارایه دهیم،
چون این دو جواب دقیق در کاربردهای عملی شکست می خورند. مثلا زمانی که ورودی تابع f(s) دارای خطاهای کوچک باشد مانند داده های تجربی که خطا دارند. یا زمانی که عملگر انتگرال، بدوضع یا بی کران باشد. به عبارت دیگر خطاهای کوچک در داده های ورودی ممکن است باعث به وجود آمدن خطاهای بزرگ در جواب بدست آمده باشد.

روش حل:
در این بخش تمرکزمان را می گذاریم روی معادله ۱ و معادله ۲ هم با همین متد ارایه شده به راحتی محاسبه می شود.
در ابتدا حالتی را فرض می کنیم که ۰=(۰)f .
f(t) نیز در بازه ی دلخواه پیوسته و مشتق پذیر است.
اگر (n+۱) امین مرتبه مشتق Ø(s)وجود داشته باشد می توانیم بسط تیلورش را تا مرتبه nام به صورت زیر بنویسیم:

$$\emptyset(t) = \emptyset(s) + \emptyset'(s)(t-s) + \cdots + \emptyset^{(n)}(s)\frac{(t-s)^n}{n!} + \emptyset^{(n+1)}(\xi)\frac{(t-s)^{n+1}}{(n+1)!}$$

ξ مقداری است بین t و s و به راحتی نشان داده می شود که $\emptyset^{(n+1)}(\xi)\frac{(t-s)^{n+1}}{(n+1)!}$ باقی مانده لاگرانژ است. برای n هایی به اندازه کافی بزرگ، مقدارش بسیار ناچیز است و نیز $\emptyset^{(n+1)}_{(x)}$ به طور یکنواخت کران دار است، پس میتوانیم از این مقدار در بسط صرف نظر کنیم. حال داریم:

$$\emptyset(t) \approx \emptyset(s) + \emptyset'(s)(t-s) + \cdots + \emptyset^{(n)}(s)\frac{(t-s)^n}{n!}$$

$$\int_0^s \frac{\left(\emptyset(s) + \emptyset'(s)(t-s) + \cdots + \emptyset^{(n)}(s)\frac{(t-s)^n}{n!}\right)}{(s-t)^v}dt = f(s)$$

$$\int_0^s \frac{\emptyset(s)}{(s-t)^v}dt + \int_0^s \frac{\emptyset'^{(s)}}{(s-t)^v}(t-s)dt + \cdots +$$

$$+ \int_0^s \frac{\emptyset^{(n)}(s)(t-s)^n}{(s-t)^v\, n!}dt = f(s)$$

$$\int_0^s \frac{\emptyset(s)}{(s-t)^v}dt = \emptyset(s)\int_0^s (s-t)^{-v}dt = \frac{\emptyset(s)(s-t)^{1-v}}{1-v}\Big|_0^s$$

$$= -\emptyset(s)\frac{s^{1-v}}{1-v} \int_0^s \frac{\emptyset'(s)}{(s-t)^v}(t-s)dt = \emptyset'(s)\int_0^s -(s-t)^{-v+1}dt$$

.
.
.

$$\int_0^s \frac{\emptyset^{(n)}(s)}{(s-t)^v}\frac{(t-s)^n}{n!}dt = (-1)^n\frac{\emptyset^{(n)}(s)}{n!}\frac{s^{n+(1-v)}}{n+(1-v)}$$

$$-\emptyset(s)\frac{s^{1-v}}{1-v} + \emptyset'(s)\frac{s^{1+1-v}}{1+1-v} + \cdots + \emptyset(s)^{(n)}\frac{s^{j+1-v}}{(j+1-v)j!} = f(s)$$

قرار می دهیم: $k(s)_{(0,j)} = \frac{(-1)^j s^{j+1-v}}{(j+1-v)j!} \qquad j = 0,1,\dots,n$

حال داریم:

$$k(s)_{(0,0)}\emptyset(s) + k(s)_{(0,1)}\emptyset'(s) + \cdots + k(s)_{(0,n)}\emptyset^{(n)}(s) = f(s)$$

پس معادله انتگرال آبل تبدیل شد به معادله ی خطی از Ø(s) ها و ما باید به طریقی این Ø(s) ها را برای حل معادله به دست بیاوریم.
(این بسط تیلور که از مرتبه n هست برای چند جمله ای ها از درجه n و کمتر، جواب دقیق بدست می آورد).
برای محاسبه ی Ø(s) ها این روند را ادامه می دهیم:
ابتدا از طرفین معادله (۱) انتگرال بر حسب s میگیریم:

$$\int_0^x \int_0^s \frac{\emptyset(t)}{(s-t)^v}\,dt\,ds = \int_0^x f(s)\,dt$$

$$\frac{1}{1-v}\int_0^s \emptyset(t)(s-t)^{1-v}\,dt = \int_0^s f(t)\,dt$$

دوباره بسط تیلور را برای Ø(t) نوشته و در معادله بالا جایگزاری می کنیم،داریم:

$$k(s)_{(1,0)}\emptyset(s) + k(s)_{(1,1)}\emptyset'^{(s)} + \cdots + k(s)_{(1,n)}\emptyset(s)^{(n)} = \int_0^s f(t)dt$$

$$k(s)_{(1,j)} = \frac{(-1)^j s^{j+2-v}}{(j+2-v)(1-v)j!} \quad j=0,1,\dots,n$$

حال اگر این روند را i بار $1\le i\le n$ تکرار کنیم به عبارت زیر میرسیم:

$$k(s)_{(i,0)}\emptyset(s) + k(s)_{(i,1)}\emptyset'(s) + \cdots + k(s)_{(i,n)}\emptyset^{(n)}(s) = f_{(i)}(s)$$

$$k(s)_{(i,j)} = \frac{(-1)^j s^{1+i+j-v}}{(1-v)\dots(i-v)(1+i+j-v)j!} \quad i = 2,\dots,n$$

$$a_n(x)y^n + a_{n-1}y^{n-1} + \ldots + a_1(x)y^{+}a_0(x)y = F(x)$$

معادله دیفرانسیل معادله‌ای است بیانگر یک تابعی از یک یا چندین متغیر وابسته و مشتقهای مرتبه های مختلف آن متغیرها. بسیاری از قوانین عمومی طبیعت (در فیزیک، شیمی، زیست‌شناسی و ستاره‌شناسی) طبیعی‌ترین بیان ریاضی خود را در زبان معادلات دیفرانسیل می‌یابند. کاربردهای معادلات دیفرانسیل همچنین در ریاضیات، بویژه در هندسه و نیز در مهندسی و اقتصاد و بسیاری از زمینه‌های دیگر علوم فراوان‌اند. معادلات دیفرانسیل در بسیاری پدیده های علوم رخ می دهند. هر زمان که یک رابطه بین چند متغیر با مقادیر مختلف در حالت ها یا زمان های مختلف وجود دارد و نرخ تغییرات متغیرها در زمان های مختلف یا حالات مختلف شناخته شده است میتوان آن پدیده را با معادلات دیفرانسیل بیان کرد.

به عنوان مثال در مکانیک، حرکت جسم بوسیله سرعت و مکان آن در زمان های مختلف توصیف می شود و معادلات نیوتن به ما رابطه بین مکان و سرعت و شتاب و نیروهای گوناگون وارده بر جسم را میدهد. در چنین شرایطی می توانیم حرکت جسم را در قالب یک معادله دیفرانسیل که در آن مکان ناشناخته جسم تابعی از زمان است بیان کنیم.

شاخه بندی: متدهای حل معادلات دیفرانسیل بسیار مرتبط با نوع معادله هستند. معادلات دیفرانسیل را به طور کلی به دو دسته می توان تقسیم کرد.

معادلات دیفرانسیل عادی: در این نوع معادلات تابع جواب دارای تنها یک متغیر مستقل است.

معادلات دیفرانسیل جزیی: در این نوع معادلات تابع جواب دارای چندین متغیر مستقل می باشد.

هر دو نوع این معادلات را می توان از دیدگاه خطی یا غیر خطی بودن تابع جواب هم دسته بندی کرد.

معادلات دیفرانسیل مشهور: قانون دوم نیوتن در مکانیک، معادلات همیلتون در مکانیک کلاسیک ،معادلات ماکسولدر الکترو مغناطیس، معادلات پواسن، مسئله منحنی کوتاه‌ترین زمان، فرمول انیشتین، قانون گرانش نیوتن، معادله موج برای تار مرتعش، نوسانگر همساز در مکانیک کوانتومی، معادله موج برای غشای مرتعش، معادلات شکار و شکارچی، مکانیک غیر خطی، مسئله مکانیکی آبل.

نوع(عادی یا جزئی): معادله شامل متغیر مستقل x ، تابع $y = f(x)$ و مشتقات f را یک معادله دیفرانسیل عادی می‌نامیم.معادله ای متشکل از یک تابع مجهول با بیش از یک متغیر مستقل همراه با مشتقات جزئی آن معادله دیفرانسیل جزئی می نامیم.

مرتبه :که عبارت است از مرتبه مشتقی که بالاترین مرتبه را در معادله دارد.

درجه: نمای بالاترین توان مشتقی که بالاترین مرتبه را در معادله دارد، پس از حذف مخرج کسرها و رادیکالهای مربوط به متغیر وابسته و مشتقاتش. معمولا یک معادله دیفرانسیل مرتبه n جوابی شامل n ثابت دلخواه دارد، این جواب را جواب عمومی می‌نامند.

ساختار:معادلات دیفرانسیل ساختارهای متفاوتی هستند و هر ساختار ویژگیهای متفاوتی دارد:

معادلات مرتبه اول از درجه اول

با متغیرهای جدایی پذیر

همگن

خطی (برنولی)

با دیفرانسیلهای کامل

معادلات مرتبه دوم

معادلات خطی با ضرایب ثابت: الف) همگن ب) ناهمگن.

تکنیکهای تقریب زدن: الف) سریهای توانی ب) روشهای عددی.

$$f_{(i)}(s) = \begin{cases} f(s) & i = 0 \\ \dfrac{1}{(i-1)!}\displaystyle\int_0^s (s-t)^{i-1} f(t)\,dt & i \neq 0 \end{cases}$$

این معادلات خطی $\emptyset(s), \emptyset'(s), \ldots, \emptyset^{(n)}(s)$ که برای n+۱ تابع مجهول هست را به صورت زیر بازنویسی می کنیم:

$$k_{nn}\overline{\emptyset_n} = f_n$$

$$k_{nn} = \begin{bmatrix} k_{(0,0)}^{(s)} & \cdots & k_{(0,n)}^{(s)} \\ \vdots & \ddots & \vdots \\ k_{(m,0)}^{(s)} & \cdots & k_{(m,n)}^{(s)} \end{bmatrix}$$

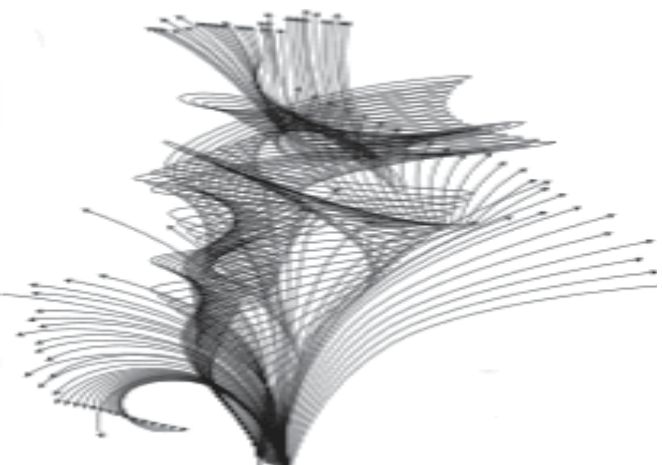
$$\overline{\emptyset_n}(s) = \begin{bmatrix} \overline{\emptyset}(s) \\ \overline{\emptyset}'(s) \\ . \\ . \\ . \\ \overline{\emptyset}^{(m)}(s) \end{bmatrix}$$

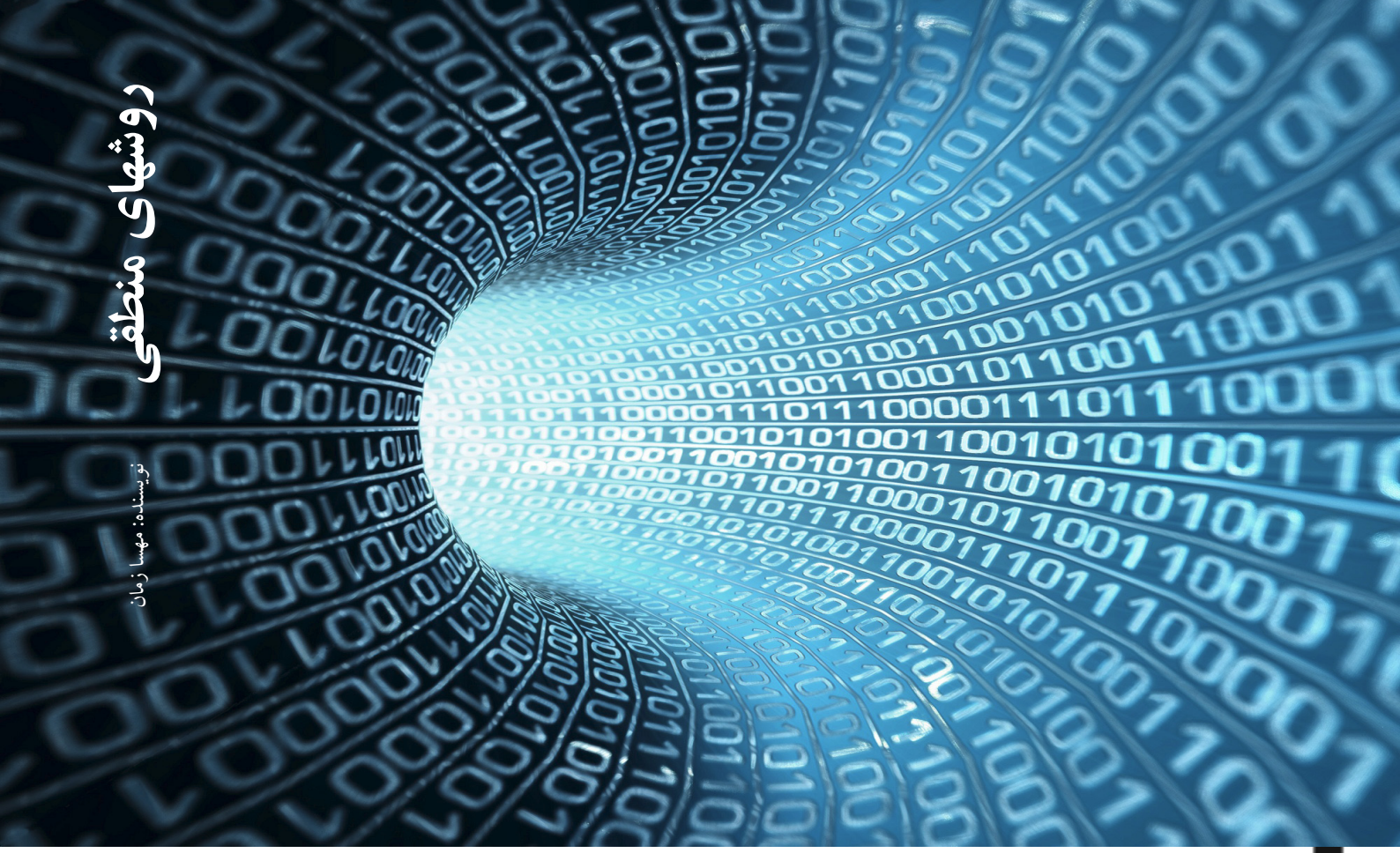
$$f_n(s) = \begin{bmatrix} f(s) \\ f_1(s) \\ . \\ . \\ . \\ f_n(s) \end{bmatrix}$$

حال به راحتی و با کمک قواعد کرامر دستگاه را حل کرده و $\emptyset^{(j)}$ ها را بدست می آوریم:

$$f_n(s) = \begin{bmatrix} f(s) & K_{(0,1)}(s) & \cdots & K_{(0,m)}(s) \\ & \vdots & \ddots & \vdots \\ f_n(s) & K_{(n,1)}(s) & \cdots & K_{(n,m)}(s) \end{bmatrix}$$

منبع: approximate solution of abel integral wquation
Li Huang,Yong Huang, Xian-Fang Li





نویسنده: مهسا زمان

منطق BAN و توسعه های آن

شاید بتوان گفت که مطالعه ی جدی درستی یابی صوری پروتکلهای رمزنگاری با مقاله ای توسط Needham و Abadi، Burrows آغاز شد.این مقاله یک منطق برای توصیف و درستی یابی پروتکلهای رمزنگاری ارائه داد که به منطق BAN (ابتدای نام نویسنده های مقاله) مشهور شد.

در حقیقت این منطق دارای یک ساختار نحوی و دستگاه استنتاجِ همراه آن بوده که با اندیشه ی معنایی مناسب برای پروتکلهای رمزنگاری طراحی شده است.

به هر حال مقاله ی اصلی هیچ ساختار صوری معنایی ای ارائه نکرده است . بنابراین اثباتی در مورد تمامیت یا صحت دستگاه استنتاج آن هم وجود ندارد.

نشریه علمی - دانشجویی رادیکال ۲
پاییز و زمستان ۹۳- شماره ۱۳

BAN برای کارکردن با پروتکل های رمزنگاری نمادهای جدید و قوانین استنتاج آنها را پیشنهاد کرده که خلاصه ای از آن در ادامه می آید:

۱- $P \mid\equiv X$

عامل pپیام xرا باور دارد. (BAN عامل یک منطق باور است)

۲- $P \lhd X$

عامل pپیام xرا میبیند ؛به عنوان مثال روی شبکه xرا در یافت میکند.

۳- $P \mid\sim X$

عامل pیک بار (مشخص نیست در چه زمانی)پیام xرا فرستاده است.

۴- $P \Rightarrow X$

عامل pصاحب پیام xاست ، برای مثال xکلید عمومی p است.

۵- $\#(X)$

پیام xتازه است،مثلا xیک مقدار نمان است.

۶- $p \overset{k}{\leftrightarrow} Q$

عامل های pوQ کلید kرا به اشتراک دارند.

۷- $\overset{k}{\rightarrow} p$

عامل pکلید عمومی kرا در اختیار دیگران گذاشته است.

۸- $p \overset{x}{\Leftrightarrow} Q$

عامل ها pوQپیام های محرمانه ی Xرا به اشتراک دارند.

۹- $\{X\}_k$

پیام xتوسط کلید kرمز شده است.

۱۰- $(X)_r$

پیام xبا پیام Yادغام شده است،مثلا توسط پیام Yامضا شده است.

همانطور که در نحوِ منطق BAN دیده میشود زمان مدل نمی شود، تنها «بعد» و «قبل» معنی دارند.

این رو اصولاً BAN نمی تواند مشکلات همزمانی یا جابجایی قدم های پروتکل را توصیف کرده و تشخیص دهد. اما تمهیدات لازم برای کارکردن با رمزنگاری نامتقارن اندیشیده شده است و مقاله ی اصلی مثالی از آنها را هم شامل میشود. در زیر چند نمونه از قانونهای استنتاج BAN را میبینیم:

$$\frac{p \mid\equiv Q \overset{r}{\Leftrightarrow} p, p \lhd (x)_r}{p \mid\equiv Q \mid\sim X} \qquad [29]$$

این قانون بیان ریاضی این مطلب است که اگر عامل P باور داشته باشد که پیام محرمانه ی Yرا با عامل Qبه اشتراک دارد و پیام Xرا در حالی که با Y امضاء شده دریافت کند، به این باور خواهد رسید که

عامل Qزمانی پیام Xرا فرستاده است.

$$\frac{p|\equiv(x)\ ,p|\equiv Q|\sim X}{p|\equiv Q|\equiv X} \quad (۲)$$

اگر عامل pباور داشته باشد که پیام X تازه است و بداند که زمانی عامل Qانرا فرستاده ،به این باور میرسد که عامل Q هم پیام Xرا در همین زمان باور دارد.

هدف این است که در نهایت قضیه ای در مورد سطح باور طرفین پروتکل به یک پیام یا کلید مشترک (برای کاربردهای تصدیق هویت) اثبات شود. معمولاً قضایای زیر مورد توجه قرار میگیرند:

$$\begin{cases} A| \equiv A \overset{k}{\Leftrightarrow} B \\ B| \equiv A \overset{k}{\Leftrightarrow} B \end{cases}$$

یعنی عامل های A,Bبه این باور برسند که کلید یا پیام kرا به اشتراک دارند. که کلید یا پیام B و A و یا قضیه ی زیر:

$$\begin{cases} A| \equiv B| \equiv A \overset{k}{\Leftrightarrow} B \\ B| \equiv A| \equiv A \overset{k}{\Leftrightarrow} B \end{cases}$$

یعنی طرفین در مورد سطح باور طرف مقابل هم به باور برسند.

این قانون ها از یک پیش زمینه ی فکری در مورد پروتکل های تصدیق هویت نشأت گرفته اند. اما نداشتن ساختار صوری معنایی منجر به این میشود که کاربرانی که با این قانون ها مواجه میشوند آنها را مطابق با ادراک خودشان به کار برند. . به این ترتیب Nessettمثالی ارائه کرد که نشان دهد که چطور میتوان با استفاده از BANثابت کرد که یک پروتکل ناامن ،امن است.

پس BAN یک ساختار درست نیست (اینکه یک پروتکل نا امن است در لایه ی فرازبانی BAN بدست می آید چرا که اصولا BAN دارای ساختار معنایی برای تعریف امنیت نیست). سپس Snekkenes نشان داد که مثال Nessett حالت ویژه ای است که تفاوت درک کاربر از قوانین استنتاج BAN را آشکار می کند. به همین ترتیب Monniaux اثبات کرد که BAN تصمیم پذیر است (اینجا هم چون BAN ساختار معنایی ندارد، اثبات تصمیم پذیری بی معنا می نماید، آنچه Monniaux نشان داده این است که همواره یک الگوریتم عقبگرد برای یافتن اثبات یک نتیجه در دستگاه استنتاج BAN وجود دارد).

ابزار نرم افزاری گوناگونی برای تولید خودکار اثبات برای قضایای BAN آماده شده و یا اختصاصاً نوشته شده اند که از جمله آنها میتوان به SPEAR، EVES و Jape اشاره کرد.

مشکلات منطق BAN و جذاب بودن ایده ی آن باعث شد که کارهای پژوهشی بسیاری در پیروی از آن انجام شوند. یکی از مشهورترین این تلاشها، منطقی بود که Yahalom, Gong و Needham ، ارائه کردند؛ این منطق قانونهای استنتاج BAN را توسعه می داد و به منطق GNY معروف شد .

ابزار نرم افزاری گوناگونی برای خودکارسازیِ GNY معرفی شدند؛ همچنین نشان دادند که این منطق هم درست نیست. Tuttle و Abadi به منظور رفع مشکلات BAN یک ساختار معنایی به آن افزودند که به منطق AT مشهور شد، Van Oorschot هم BAN را برای کارکردن با پروتکلهای موافقت کلید توسعه داد که به منطق VO مشهور شد. پراکندگی این کارها باعث شد که VanOorschot Syverson منطقهای VO و BAN، GNY، AT را تحت نام منطق SVO جمع کرده و یک ساختار معنایی برای آن ارائه دادند و نشان دادند که ساختار استنتاج SVO درست است یک ابزار نرم افزاری هم بر SVO اساس توسعه یافته است.

یکی از منطقهایی که بر اساس BAN بنا شده و در درستی یابی پروتکلهای تجارت الکترونیک (SET Payword) به کار رفت AUTLOG است. این منطق قوانین استنتاج جدیدی به BAN افزوده که (طی یک ساختار معنایی در لایه ی فرازبانی) همخوانی این قوانین با BAN اثبات شده است.

همچنین Boyd و Mao منطق BAN به همراه ایده آل سازی صوری پروتکل را توسعه داده و بخشی از مشکلات BAN ناشی از نداشتی ساختار معنایی (حمله ی Nessett) را حل کردند.

تلاشهایی هم برای افزودن مفهوم زمان به BAN انجام گرفت. از جمله Benerecetti و بقیه منطق BAN را با یک منطق زمانی تلفیق کرده و الگوریتم وارسی مدل مربوط به آن را هم ارائه کرده اند. همچنین Syverson عملگرهای زمانی را به BAN افزوده و ساختار معنایی آن را هم طرح کرد .

یک منطق دیگر که بر اساس BAN توسعه یافت RV است.

RV از این نظر اهمیت دارد که با یک دستگاه اثبات خودکار می آید. ایده این است که یک نمایش متناهی از یک نظریه (نه لزوماً متناهی) در اختیار داشته باشیم که بتواند در تصمیم گیری عضویت یک گزاره در آن به ما کمک کند و خودش هم به صورت کارآیی قابل محاسبه باشد. این نمایش متناهی «نظریه ی متناهی کارآ ۱» نامیده میشود.

«اشباع نظریه ۲» یکی از روشهای تولید یک نظریه ی متناهی کارآ است که ابتدا برای منطق مرتبه اول پیشنهاد شد. همانطور که از تصمیم ناپذیری منطق مرتبه اول انتظار داریم، روش اشباع نظریه هیچ اطمینانی در مورد پایان پذیری ۳ الگوریتم تولید نظریه ی متناهی کارآ برای منطق مرتبه اول ارائه نمی دهد.

الگوریتمی که Kindred در رساله ی دکترایش ارائه میدهد تولید نظریه ۴ نام دارد و در مورد گروه خاصی از نظریه ها به کار میرود. تحت شرایط خاصی برای نظریه ی اصلی، این امکان وجود دارد که نظریه ی متناهی کارآیی متناظر با آن تولید شود؛ به طور بسیار مختصر باید یک زیر مجموعه ی ویژه از قوانین استنتاج انتخاب شده و تنها گزاره هایی در نظریه ی متناهی کارآ قرار داده شوند که یک درخت استنتاج منتهی به یکی از قانونهای آن زیر مجموعه داشته باشد. معمولاً قانونهایی در این مجموعه ی ویژه قرار میگیرند که اندازه-گاه باشند ادعای مهم Kindred ۶. این است که BAN و یک نسخه ی بهبود یافته ی آن از نظر معنایی (یعنی RV) شرایط اعمال روش تولید نظریه را دارند و یک بسته ی نرم افزاری برای پیاده سازی ایده ی فوق ارائه میکند.

همانطور که در گفته های فوق مشهود است، بسیاری از توسعه های BAN ساختار معنایی به آن افزودند .

Accorsi و بقیه ساختار معنایی ویژه ای برای BAN طرح کرده اند که سعی می کند مسأله ی «همه چیز دانی » را در مورد این منطق حل کند. موضوع از این قرار است که در بررسی های نظری هنگامی که میگوییم یک عامل مجموعه ای از گزاره ها را میداند، به طور ضمنی فرض میشود که نظریه ی حاصل از آن مجموعه (نظریه ی حاصل از یک مجموعه از گزاره ها، مجموعه ای است از گزاره ها که با اعمال نامتناهی قوانین استنتاج بر روی اعضای مجموعه ی اصلی بدست می آید) را هم می داند. در حالی که به علت محدودیت منابع و زمان در سیستمهای رایانه ای (و حتی انسانی)این فرض درست نیست، به این معنی که یک رایانه همه ی آنچه را که میتواند بداند، نمیداند.

از آنجا که این مسأله به طور جدی تری خودش را در مباحث هوش مصنوعی نشان میدهد محققین این شاخه اولین راه حل ها را برایش پیشنهاد کرده اند که از جمله ی آنها دیدگاه «هشیاری ۲» است. در دیدگاه هشیاری، دانش یک عامل به دو دسته ی دانش ضمنی و دانش صریح تقسیم میشود و حدس زدن اینکه هر کدام از آنها به چه بخشی از دانایی اشاره دارند ساده است. در همین راستا Accorsi و بقیه یک ساختار معنایی مبتنی ،بر هشیاری برای BANارائه دادند.

منطقهای دانش در برابر منطق های باور

من هرگز برای باورهایم نخواهم مرد، چراکه ممکن است در اشتباه باشم
برتراند راسل

این جمله ی راسل هرچند ممکن است کمی تلخ به نظر رسد، اما به نکته ای اشاره دارد که اساس تفاوت بین منطق های دانش و منطق های باور۱ منطق دانایی ۲ و منطق باور ۳هردو جزو منطق های وجهی بشمار میآیند، با این تفاوت که در منطق دانایی دانش یک عامل از درستی یک گزاره به معنی درستی آن است، اما در منطق های باور ممکن است یک عامل به درستی یک گزاره باور داشته باشد اما آن گزاره درست نباشد.

من
هرگز برای
باورهایم نخواهم مرد،
چراکه ممکن است در
اشتباه باشم
برتراند راسل

به طور خلاصه اگر عملگرOنماینده دانش(یا باور) یک عامل iباشد.اصل۵ زیر در منطق دانایی وجود داشته اما در منطق باور وجوبی ندارد:

$$O_i P \overset{?}{\Rightarrow} p$$

منطق BANو توسعه هایش منطقهای باور هستند و این امکان وجود دارد که منطق های دانایی هم برای مدل سازی و درستی یابی پروتکل های رمزنگاری به کار روند. به نظر می رسد مهمترین کاری که در این زمینه انجام شده مقاله ای از Syverson باشد که در آن اصولاً نوع نگاه منطقهای متفاوت به مسأله «امنیت» بررسی شده است . فرض و بحث شهودی مقاله بر این است که موضوع «۶اعتماد» (اساس تصدیق هویت) ریشه در باور دارد در حالیکه «محرمانه بودن» ریشه در دانش دارد. هر چند که به طور مستدل نمی توان این ادعا را ثابت کرد اما چندان دور از ذهن هم نیست. با این فرض، Syversonیک ترجمه ی نحوی (مسلما بدون توجه به معنا، اگر نه دو منطق یکسان میشدند) برای تبدیل هر کدام از این منطقها به دیگری ارائه میدهد. از آنجا که اثبات قضایا در منطق دانش اصولاً ساده تر از منطق باور است (تلاشی برای اثبات درستی یک گزاره بعد از اثبات دانش یک عامل نسبت به درستی آن لازم نیست)، پیشنهاد میشود که حتی منطقهای باور به منطقهای دانش ترجمه شده وفقط ابزار کار در منطق دانایی توسعه یابد. تنها نقطه تاریک استدلال فوق این است که ممکن است در یک منطق باور عبارت $OjP\& \sim P$ (نقیض اصل فوق) درست باشد، و ما نمیدانیم چطور این عبارت را در منطقِ دانایی (که چنین عبارتی همواره نادرست است) گنجانده و با آن کار کنیم. ادعای Syverson بر این است تنها مواقعی این اتفاق رخ میدهد که یک مشکل امنیتی از نوع محرمانه بودن هم وجود دارد (بر اساس مطالعات موردی که در مقاله ذکر شده است) و باز باید توسط منطق دانایی بررسی شود. او نام این موقعیت را باور نابجا گذاشته و استدلال میکند با چنین باوری حتما محرمانه بودن اطلاعات هم برقرار نخواهد بود. به این ترتیب استفاده از منطقهای دانش در درستی یابی صوری پروتکلهای رمزنگاری دارای توجیه مناسبی شد. اولین آنها منطق CTK. ۵ است که توسط Bieber ارائه شد. سپس Carlsénیک کاربرد جذاب از این منطق را نشان داد؛ به این صورت که یک حفره امنیتی در لایه ی پیاده سازی یک پروتکل را تشخیص داد.. هر چند که این حفره تا حدی ساختگی بوده و به راحتی به حالت کلی قابل تعمیم نیست (مشکل مورد بحث ناشی از عدم تفکیک انواع دادهها ۲ در پیامهاست) اما باز هم تنها نمونه ای است که یک مدل منطقی در لایه ی پیاده سازی پیش میرود. Carlsen همچنین ابزار تبدیل خودکار توصیف پروتکل به ساختار نحوی منطق CTK ۵ را هم ارائه داد.

منطق KPL یکی دیگر از منطق های دانایی است که همزمان با CTK ۵ توسط Syverson ارائه شده است.

هرچند که KPL همراه ساختار صوری معنایی مربوط به آن آمد اما اثباتی در مورد صحت و تمامیت آن وجود ندارد . یک رویکرد تلفیق منطق دانش با احتمالات هم توسط Syverson Gray مطالعه شده است. گذشته از بحثهای Syverson در مورد استفاده از منطق دانایی بجای منطق باور، به نظر میرسد که یک دیدگاه محافظ کارانه استفاده از هر دو منطق به صورت تلفیقی است مشروط به این که حجم محاسبات مورد نیاز دچار انفجار نشود. جالب است که اولین منطق تلفیقی پیش از همه ی این داستان ها در سال ۱۹۸۹ توسط Moser استفاده شد ، منطق Moser یک منطق نایکنواخت نیز به شمار می آید که با معرفی عملگر «مگر۳» ارزش نایکنواخت گزاره ها را مدل میکند.

در این منطق با وجود $Oi\ p\ unless\ Oiq$ عامل i گزاره ی p را باور دارد مگر اینکه به گزاره ی q باور پیدا کند، پس باور نسبت به p ممکن است در زمان عوض شود.

منطق تلفیقی Saidha و Coffey هم در سال ۱۹۹۶برای درستی یابی پروتکلهای رمزنگاری ارائه شد. هر دو منطق فوق عملگرهای مستقلی برای باور و دانش دارند. جدول ۱ مطالب فوق را خلاصه میکند.

جدول ۱- منطق های دانایی و باور

تلفیقي	منطق دانايي	منطق باور
Moser 89	Bieber 90 (CTK5)	[110] R.V.Rangan 88
Coffey, Saidha 96	Syverson 90 (KPL)	BAN 89
	ديدگاه احتمالاتي Syverson 95	توسعه هاي BAN

منطقهای دیگر

یکی از انتقاداتی که ممکن است بر استفاده از منطق های خاص منظوره وارد باشد، نداشتن سابقه ی نظری کافی و به تبع آن نداشتن ابزار نرم افزاری کارآ ست. کمتر منطقدان حرفه ای وجود دارد که منطق BAN را مطالعه کرده باشد و شاید مشکلات معنایی BAN از اینجا باشد.هرچند که شرایط در حال تغییر است اما استفاده از منطقهای متعارف تدبیر نادرستی به نظر نمیرسد. البته نباید از نظر دور کرد که بیان و توصیف مسأله در یک منطق چند منظوره ممکن است به سادگی BAN نباشد. منطق زمانی در زمینه درستی یابی پروتکلها سابقه ی طولانی دارد و تلاش برای استفاده از آن در مورد پروتکلهای رمزنگاری ابتدا توسط McLean و Grayمطرح شد. به این ترتیب، مستقیماً پس زمینه ی نظری وحمایت نرم افزاری منطق زمانی شامل حال پروتکلهای امنیتی میشود. همچنین Huimaو Aura منطق S4n را که یک منطق چندوجهی است وارد این تحقیقات کردند. در سال ۱۹۹۹ ایده ی استفاده از قطعه ای از منطق مرتبه اول برای این منظور مطرح شد، و در سال ۲۰۰۳ نشان داده شد که آن قطعه از منطق مرتبه اول تصمیم پذیر است. به همین ترتیب Delzanno از منطق شهودگرای hhf و نرم افزار lambda-prolog برای توصیف و درستی یابی پروتکلهای امنیتی استفاده کرد.

منطق بازنویسی یک ساختار منطقی درست و کامل است که ایده ی تغییر را در خود دارد. از نظر منطق بازنویسی هر قانون استنتاج معادل با بازنویسی یک عبارت با عبارت معادلش طبق قانون است. از این رو بسیاری از منطق های دیگر به نوعی یک منطق بازنویسی به شمار می آیند. حتی حساب لاندا ۵قابل بیان در قالب یک منطق بازنویسی است . بسته های نرم افزاری بسیاری برای پیاده سازی منطق بازنویسی وجود دارند که از میان آنها daTac توسط Jacquemard و بقیه (به همراه یک ابزار تولید خودکار توصیف صوری) Maude توسط Denker وبقیه برای درستی یابی پروتکل های رمزنگاری به کار رفته اند. در کنار این روشها در سال ۱۹۹۳ یک ساختار صوری (مانند مدلDolev-Yao) برای مدل سازی پروتکلهای رمزنگاری توسط Lam و Wooارائه شد که در برخی تحقیقات بعدی به کار گرفته شد. آنها برای بررسی امنیت از ایدههای «تناظر» و «محرمانه بودن» استفاده کردند. تناظر به این معنی به کار رفت که در یک پروتکل تصدیق هویت همه ی دست اندر کاران باید در پروتکل قفل شده و تاانتهای آن حضور داشته باشند. برای عنوان مثال اگر تصدیق هویت کننده به انتهای وظایفخودش طبق پروتکل می رسد، طرف تصدیق هویت شونده باید حضور داشته و به مرحله ی آخر وظایف خودش رسیده باشد. با توجه به این ایده، آنها یک دستگاه استنتاج برای اثبات امنیت پروتکلهای رمزنگاری ارائه کردند.

منبع: پایان نامه ارشد گرایش علوم کامپیوتر،
نگارش محمددشتی،استاد راهنما دکتر محمد اردشیر

پالیندروم چیست؟

پالیندروم (واروخوانه یا قلب مستوی هم گفته می شود) به کلمه، جمله (رشته ای از کلمات) یا اعدادی گفته می شود که از دو طرف (راست به چپ و چپ به راست) دقیقا به یک شکل خوانده می شوند. (در واقع از دو طرف متقارن هستند.)
مثلا واژه «رادار» یا «بابک و کباب» و عدد «۱۴۵۶۵۴۱» همگی مثالهایی از پالیندروم هستند.
واژه پالیندروم، از دو کلمه با ریشه ای یونانی بوجود آمده است: پالین (πάλιν)، به معنای مجدد، تکرار، و دروموس (δρόμος) به معنای راه و مسیر.
یکی از طولانی ترین متون پالیندروم، دارای ۱۷۲۵۹ واژه است. .
عدادی واژه‌های پالیندروم فارسی (یا متداول در فارسی) در اینجا آمده است:

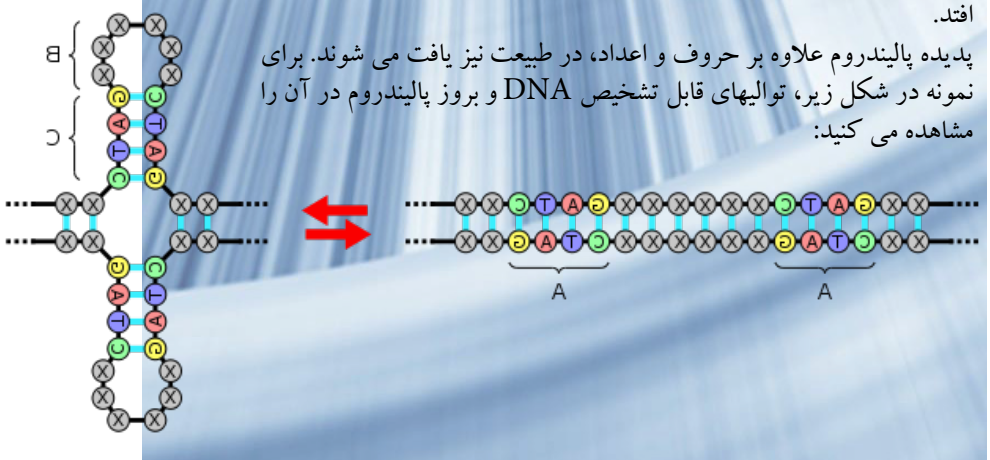
دو حرفی:
دَد، کَک، شِش، شُش، سُس

سه حرفی:
نان، دود، توت، درد، گرگ، داد، کشک، کلک، کتک، کیک، کپک، کوک، کَبک، کمک، کاک (نوعی شیرینی)، دید، دهد، تخت، بمب، پمپ، پیپ، موم، گنگ، شوش، دزد، همه، ساس، شپش، تشت، لال، اما، یکی، آیا، آرا، تبت، لیل، قُرُق، میم، نون، واو

بیش از سه حرف:
رادار، مادام، داماد، همهمه

در متون قدیمی به پدیده پالیندروم، مقلوب مستوی، بالانعکاس و جناس مالایستحیل هم می گفتند. چند نمونه قلب مستوی در متون قدیمی پارسی:
دربیت زیر، هر مصرع یک قلب مستوی (پالیندروم) می باشد:
شکر بترازوی وزارت برکش / شو همره بلبل بلب هر مهوش
مثال قلب مستوی (پالیندروم) در یک بیت:
رامش مرد گنج باری و قوت تو قوی را بجنگ در مشمار.
مثال قلب مستوی (پالیندروم) در کل یک غزل:
آرام برای حور دارم یارا
زین شوخ مراد ما دمی مرگ روا
امشب می و کنجی و همه شب همره
خوش ناز منی بلا مجو مرگ مرا
آیم بر حرب زور ای مه ناخوش
شو خانه میا روز بر حرب میا
آرم کرم و جمال بینم زآن شوخ
هر مه بشیم هیچ نگویم بشما
آور که می مدام دارم خوش نیز
آرای مراد روح یا رب ما را.

پالیندروم را برای اعداد هم داریم، سال ۲۰۰۲ یک سال پالیندروم بود. احتمالا اگر شما سال ۲۰۰۲ را به یاد دارید، ممکن است تجربه زندگی در سال ۱۹۹۱ را هم داشته باشید.
دو سال پالیندروم متوالی گذشته که ممکن بوده یک نفر هر دوی آنها را تجربه کرده باشد بر می گردد به سال ۹۹۹ و ۱۰۰۱ میلادی! آیا فکر می کنید به اندازه کافی عمر خواهید کرد که یک بار دیگر، یک سال پالیندروم را تجربه کنید؟ در مورد سال ۲۱۱۲ صحبت می کنیم!(البته اگر از سال شمسی هم استفاده کنیم، باید تا سال ۱۴۴۱ منتظر بمانیم!)
بد نیست بدانید اگر فردی می خواهد دو سال پالیندروم متوالی دیگر را تجربه کند، باید تا سال ۲۹۹۲ و ۳۰۰۳ میلادی، صبر کند!!! این قضیه تقریبا هر ۱۰۰۰ سال یکبار اتفاق می افتد.
پدیده پالیندروم علاوه بر حروف و اعداد، در طبیعت نیز یافت می شوند. برای نمونه در شکل زیر، توالیهای قابل تشخیص DNA و بروز پالیندروم در آن را مشاهده می کنید:



مقاله رمزهای بیولوژیکی

مترجم: مهسا زمان

با تشکر از دکتر اسکندری و دکتر زارع دانشگاه امیر کبیر

امروزه تکنولوژی های شبکه بسیار بهبود یافته اند به طوریکه مردم برای فرستادن یا گرفتن انواع مختلفی از داده های دیجیتال تحت اینترنت به دوردستها به تسهیلات بیشتر و بیشتری دسترسی دارند.
به هر حال اینترنت مکانی عمومی است و برای انتقال داده ها کانال نا امنی است. هم چنین اطلاعات مهم در حالی که از طریق اینترنت ارسال می شوند باید به یم فرم غیرقابل خواندن تبدیل شوند به طوری که فقط گیرنده ی مورد نظر بتواند آنها را بخواند. متد های مختلف رمزنگاری و رمزگشایی از دوران باستان مورد استفاده قرار گرفته اند . امروزه برای رمزنگاری و رمزگشایی تکنیک های بیولوژیکی به کار گرفته می شوند.

رمزهای وراثتی :

دیدیم که DNA ماده ی ژنتیک و محل ذخیره سازی اطلاعات است. اطلاعات در DNA به صورت رمز ذخیره شده اند منظور از رمز علایمی است که از آن ها برای ذخیره سازی و انتقال اطلاعات استفاده می شود مثلا زبان فارسی ۳۲ علامت رمز (حرف) دارد.

می دانید که ملکول DNA ملکول بسیار بلندی است و در ساختار آن چهار نوع نوکلئوتید به کار رفته است بنابراین می توان گفت که زبان ملکول DNA به صورت یک الفبای چهار حرفی (A, C, T, G) است که هر حرف آن نشان دهنده ی یک نوع نوکلئوتید است.

از اطلاعات ژنتیک برای ساختن پروتئین استفاده می شود پروتئین ها از ۲۰ نوع آمینو اسید ساخته شده اند و هر پروتئین توال آمینواسیدی مخصوص به خود را دارد . در واقع رمزهای موجود در DNA باید به نحوی تعیین کننده ی نوع و ترتیب آمینواسیدهای پروتئین ها باشند .

اگر هر نوکلئوتید علامت رمز یک آمینو اسید باشد باز های A, C, G, T علامت های رمز چهار نوع آمینواسید می شوند . بنابر این فقط چهار نوع آمینو اسید رمز خواهند داشت . بدیهی است که رمز یک حرفی جوابگوی ۲۰ نوع آمینو اسید نخواهد بود در صورتی که رمز دو حرفی باشد فقط ۱۶ نوع آمینو اسید علامت رمز خواهند داشت بنابراین رمز دو حرفی نیز جوابگوی ۲۰ نوع آمینو اسید نخواهد بود در صورتی که رمز سه حرفی باشد ۶۴ رمز سه حرفی به دست می آید که بیشتر از تعداد رمز لازم برای ۲۰ نوع آمینواسید است در اینصورت یک آمینواسید ممکن است بیش از یک رمز داشته باشد در واقع رمز های نوکلئیک اسیدها سه حرفی هستند.

یک تکنیک رمزنگاری ساده بر پایه ی دنباله های آمینواسد پروتئین:

اخیرا تکنیک های بیولوژیکی پرطرفدار شده اند چون برای انواع متفاوتی از کاربردها مثل پروتکل های احراز هویت ، بیوشیمی و رمزنگاری به کار برده می شوند .

بیوانفورماتیک در پایگاه داده های ملوکولی نقش مهمی دارد . رمزگذاری کردن داده های محرمانه در دنباله های پپتیدی یا دنباله های آمینو اسید تبدیل به یکی از موضوعات پژوهشی مهم و جالب شده است . این مقاله یک روش رمزنگاری قابل اعتماد و امن را نشان می دهد که پیام را به یک دنباله ی آمینو اسید پروتئین برای ایجاد امنیت تبدیل می کند.

همانطور که می دانید آمینواسیدها ملکول هایی هستند متشکل از یک گروه آمین و یک گروه کربوکسیلیک اسید که به شکل زنجیر به هم متصل می شوند و این ترکیب بین آمینواسیدهای مختلف تغییر می کند.

عناصر کلیدی یک آمینو اسید ، کربن ، هیدروژن ، اکسیژن و نیتروژن هستند . آمینو اسیدها برای زندگی حیاتی هستند و در متابولیسم بدن کاربردهای زیادی دارند . آمینواسیدها می توانند در دنباله های مختلفی به هم وطل شوند تا انواع بسیاری از پروتئین ها را تشکیل دهند. به طور طبیعی ۲۲ آمینو اسید در پلی پپتید ها به هم پیوسته اند که به نام پروتئینوژنتیک یا آمینو اسیدهای استاندارد خوانده می شوند و در جدول زیر نشان داده شده اند:

A	alanine	M	methionine
C	cysteine	N	asparagine
D	asparatic acid	P	proline
E	glutamic acid	Q	glutamine
F	phenylalanine	R	arginine
G	glycine	S	serine
H	histidine	T	threonine
I	soleucine	V	valine
K	lysine	W	tryptophan
L	leucine	Y	tyrosine

به علاوه دو آمینو اسید دیگر که به وسیله ی کدون های توقف یکی شده اند وجود دارد:

U	selenocystine	O	pyrrolysine

از ۲۲ دنباله ی آمینو اسیدی بالا یک کاربر می تواند به طور تصادفی یک جایگشت از میان !۲۲ جایگشت را انتخاب کند . کار حاضر در مورد یک تکنولوژی رمزگذاری کلید متقارن بحث می کند که از دنباله های آمینواسیدی بالا استفاده می کند . فرستنده یک جایگشت تصادفی از دنباله های بالا را به عنوان یک کلید انتخاب می کند و یک جدول جستجوی دینامیک را برای رمگذاری و رمزگشایی تولید می کند . از آنجایی که این الگوریتم کلید مقارن است فرستنده کلید را برا گیرنده منتقل می کند چون این کلید محرمانه است ، که باید برای هر دو عمل رمزنگاری و رمزگشایی به کار گرفته شود.

تولید کردن کلید:

۱. آلیس مجموعه ی بالا را به طور تصادفی به دو زیرمجموعه ی زیر تقسیم میکند :

i) { A , C , D , E , F , G , H , I, K , L , M , N , O , P , Q, R, S, T, W, Y, U }

ii) { V }

۲. از آنجایی که آلیس می خواهد تا اطلاعات محرمانه را به باب منتقل کند ، باب یک جایگشت تصادفی از زیرمجموعه ی اول انتخاب می کند. می گوید: یک عدد تصادفی در بازه ی { ۱ و !۲۱ } به عنوان کلید رمز انخاب کنید.

می گوید : باب جایگشت زیر را انتخاب میکند:

HGFCADILNMYTSWFERPOQU

۳. همچنین آلیس یک کاراکتر تصادفی به عنوان زیرمجموعه ی دوم انتخاب میکند.

۴. آلیس این کلید را به باب می فرستد { «, «v HGFCADILNMYTSWFERPOQU » { »

رمزگذاری :

آلیس جدول جستجوی زیر را تولید می کند که دنباله های آمینواسیدی را برای مجموعه کاراکترهای استاندارد ASKIIنشان می دهد که مقدار آنها از ۳۲ تا ۱۲۶ است .

نمایش کاراکتری آمینو اسید	کد اسکی	نمایش کاراکتری آمینو اسید	کد اسکی
Column4	Column3	Column2	Column1
O	18	H	0
Q	19	G	1
U	20	F	2
FG	21	C	3
FF	22	A	4
FC	23	D	5
FA	24	I	6
FD	25	L	7
FI	26	N	8
FL	27	M	9
FN	28	Y	10
FM	29	T	11
CH	30	S	12
CG	31	W	13
CF	32	F	14
.	.	E	15
.	.	R	16
MA	94	P	17

آلیس اکنون هر کاراکتر متن آشکار را با کمتر از دو کاراکتر نشان می دهد تا متن رمزی را تولید کند . چون باب { V } را به عنوان زیر مجموعه ی دوم انتخاب کرده ، V یک کاراکتر یکتا را در متن رمز نمایش می دهد.
آلیس متن رمزی برای هر کاراکتر را به وسیله ی کم کردن ۳۲ از مقدار کد اسکی تولید می کند و دنباله ی آمینو اسیدی را برای کاراکتر از جدول بالا به دست می آورد.
مثال: بیایید فرض کنیم آلیس میخواهد متن آشکار زیر را بفرستد:
« This is Amino-acid sequence »
روشی که آلیس متن رمزی را برای متن آشکار تولید می کند در جدول زیر نمایش داده شده است.

T	84	52	DF
h	104	72	LF
i	105	73	LC
s	115	83	NC
space	32	0	H
i	105	73	LC
s	115	83	NC
space	32	0	H
A	65	33	CC
m	109	77	LL
i	105	73	LC
n	110	78	LN
o	111	79	LM
-	45	13	W
a	97	65	ID
c	99	67	IL
i	105	73	LC
d	100	68	IN
space	32	0	H
s	83	51	DG
e	101	69	IM
q	113	81	NG
u	117	85	NO
e	101	69	IM
n	110	78	IN
c	99	67	IL
e	101	69	IM
.	46	14	F

آلیس هر دنباله ی ۲ کاراکتری را با « U » جلو می برد و هر دنباله یک کاراکتری را با V جلو می برد و متن رمز زیر را می فرستد:
DFLFLCNCVHLCNCVHCC
LLLCLNLMVWIDILLCINV
HDGIMNGNDIMLNILIMVF

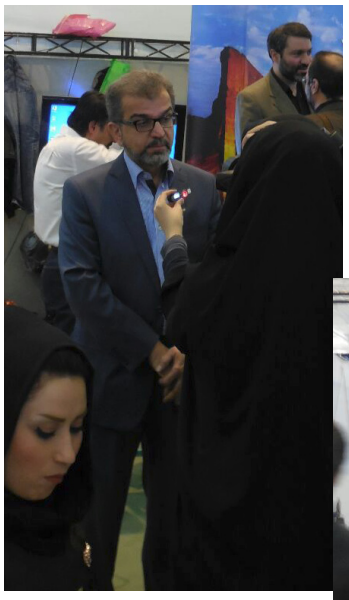
برای رمزگشایی بعد از دریافت متن رمز باب، جدول جستجو مشابهی را برای شکستن رمز تولید می کند . او رمز را به وسیله ی گرفتن ۲ کاراکتر در هر مرتبه برای رسیدن به یک کاراکتر معادل در متن آشکار می شکند و هرگاه که باب با کاراکتر V مواجه شد کاراکتر بعدی را تک کاراکتر در نظر می گیرد تا معادل آن را در متن آشکار پیدا کند.

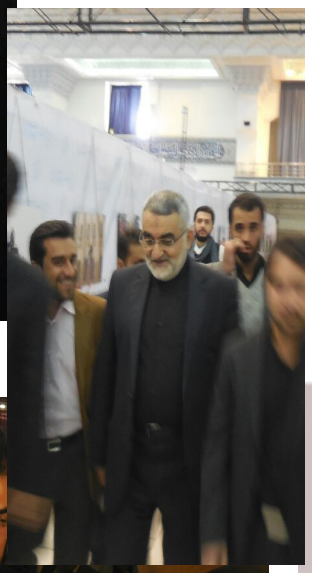
رمزنگاری کافی نیست:

منبع:پایان نامه کارشناسی رمزنگاری و امنیت شبکه
طیبه موسوی

با در دست داشتن یک ابزار پر قدرت رمزنگاری و با دانستن قابلیت های آن ابزار این امکان وجود دارد که میزان اطمینان به این فناوری در راستای برقراری و حفظ امنیت اطلاعات بالاتر رود . بنابراین خوب است که همین جا به نقطه ی گمراه کننده ی آن نیز اشاره شود. اغلب تصور می شود که رمزنگاری می تواند به عنوان یک راه حل جامع برای انواع مسائل امنیتی امروز مطرح شود و می تواند جلوی حمله و نفوذ هکرها را بگیرد اما این تصور اشتباه است و هرگز نمی توان رمزنگاری را سپری در برابر همه ی مشکلات دانست. بسیاری از نفوذگرها با آگاهی از نقاط ضعف تنظیمات پیش فرض سیستم ها ، کاستی ها و آسیب پذیری های پروتکل های شبکه و نرم افزارها ، دست به سواستفاده و نفوذ می زنندحتی برخی از ابزارها و نرم افزارهای امنیتی و رمزنگاری نیز نقاط ضعفی دارند که آنها را در برابر ذهن جستجوگر انسان تسلیم می کند.
در برابر چنین مسایلی دستان رمزنگار کاملا خالی خواهد بود و روش هایی غیر از رمزنگاری برای جلوگیری از ورود بیگانگان لازم خواهد بود. راه های بسیاری وجود دارد که به کمک آنها می توان تاثیر رمزنگاری را در سیستمی که به آن نفوذ شده است از بین برده و به طور کامل خنثی کرد. تکیه ی کامل بر رمزنگاری و در نظر نگرفتن سایر مسایل امنیتی دقیقا مثل آن است که در پشتی خانه را به قوی ترین قفل غیر قابل شکست مجهز کنید و در جلویی را به طور کامل باز بگذارید و دل گرم به قفل شکست ناپذیر خود باشید . متاسفانه اطمینان به روش های رمزنگاری مدرن در بسیاری موارد موجب شده است که درباره ی سایر مسایل امنیتی که تعدادشان کم هم نیست ، غفلت شود بنابراین با وجود پیشرفت های بزرگ در رمزنگاری و طراحی روش های توانمند تا زمانی که سیستم ها ، بسترهای ارتباطی ، و نوع ارتباطات در حال تغییر است همواره مسایل جدیدی مطرح می شود که بدون بررسی کشف و رعایت نکات مربوط به آنها قدرت رمزنگاری و به طور کلی تر برقراری امنیت فاقد معنا خواهد بود.
پنهان سازی و رمزنگاری زمانی که نمی توان حتی به توانمند ترین روش های رمزنگاری به طور کامل اطمینان کرد شاید بتوان با استفاده از استگانوگرافی یا پنهان سازی داده در داده و بالا بردن سطح امنیت توسط آن ضریب امنیت را افزایش داد .
« بهترین روش استگانوگرافی یا پنهان ساختن فرآیندهای رمزگونه در اطلاعات بکارگیری یک ایده ی ابتکاری نامشکوک جدید است»
جمله ی بالا را بخوانید و کمی درباره ی آن تامل کنید اگر فکر می کنید این جمله به شما تنها بهترین روش پنهان سازی داده ها را می آموزد من در به کارگیری یک روش ساده ی استگانوگرافی موفق بوده ام.بار دیگر به جمله ی آغازین این بند بازگردید و حروف اول آن را در کنار هم بچینید و البته هر جا لازم دانستید بین حروف فاصله قرار دهید تا این جمله ی پنهان کشف شود :
« برای پس فردا بیا آنجا »
اگر شما قبل از گفتن من به آن جمله مشکوک شده بودید در آن صورت تلاش من برای استگانوگرافی شکست خورده به شمار می آید هر چند شانس من برای موفقیت بسیار زیاد بوده است و به احتمال زیاد اکثر قریب به اتفاق خوانندگان یک مقاله به چنین چیزی غیر از معنی جملات آن و درک مستقیم آنها توجه نمی کنند . البته این بعید نیست که خوانندگان از این پس به ادامه ی این مقاله یا حتی مقالات خاص دیگر مشکوک شوند ، بنابراین تلاش دوباره برای این کار با احتمال بیشتری به شکست خواهد انجامید.
اما مهم این است که قبل از آن هیچ شکی به این نوشته ها وجود نداشت و در صورتی که صریحا به وجود این نوع اطلاعات پنهان اشاره نمی شد و از طرفی از این کار یک هدف واقعی امنیتی را دنبال می کردم در نهایت به هدف خود یعنی انتقال اطلاعات محرمانه به مقصد می رسیدم البته همانطور که در ابتدا گفتیم این روش دیگر لو رفته و من باید این روش را تنها در جایی به کار ببرم که مطمئن باشم مخاطبان آن قبلا این مقاله را نخوانده اند یا اگر هم خوانده اند مطمئن باشم که افراد به اطلاعاتی که در اختیارشان قرار می دهم مشکوک نخواهند شد و اصولا دلیلی برای مشکوک شدن آنها وجود نداشته باشد. اما اگر بار دیگر قصد دارم اطلاعات محرمانه ی دیگری را در حامل پیدا کنم بهتر است هم در انتخاب حامل و هم در نوع پنهان سازی به روشی جدید و ابتکاری عمل کنم به طوری که آن حامل هم چنان نامشکوک باقی بماند.
حال اگر اطلاعاتی که قصد پنهان سازی آن را داریم قبلا به صورت رمز شده نیز در آمده باشد حتی در صورت شک به وجود پیام در حامل ، پیام به راحتی لو نخواهد رفت . یافتن حامل های جدید اطلاعات طراحی روش پنهان سازی کارا و استفاده از روش های رمزنگاری قدرتمند در کنار هم می تواند با افزایش سطوح امنیت ، قابلیت اطمینان را برای حفظ محرمانگی اطلاعات افزایش دهد.

گزارش
بیستمین نمایشگاه مطبوعات





بیستمین نمایشگاه مطبوعات، خبرگزاری‌ها و پایگاه‌های اطلاع‌رسانی از ۱۸ تا ۲۴ آبان ماه سال جاری در مصلای تهران برگزار شد.از آنجا که این نمایشگاه مختص خبرگزاری ها بود لذا اخبار آن نیز سریعتر از نمایشگاه های دیگر حتی نمایشگاه کتاب مخابره میشد.بازار داغ بازدید شخصیت های خبری از خبرگزاری ها داغ بود و هر آن با یک سر چرخاندن در نمایشگاه و دیدن گروه زیادی از مشایعت کنندگان کافی بود فقط پیگیر اخبار بوده باشید تا بدون دانستن نام مقام مسئول تشخیص دهید که ایشان در کدام حوزه فعالیت دارند.شناخت افراد کار آسانی بود اما دعوت از آنها برای بازدید از غرفه ی دانشگاه کاری بس دشوار بود چرا که مثل همیشه غرفه های دانشگاهی در یکی از کوچه های کم تردد واقع شده بود با این حال نمیتوان بازدید مسئولین وزارت علوم را نادیده گرفت وجا دارد از نماینده ی مردم بجنورد در مجلس شورای اسلامی هم تشکر ویژه ای داشته باشیم که در مصاحبه اش با خبرگزاری خانه ی ملت با ابراز تأسف از بی مهری نسبت به بخش های دانشگاهی در نمایشگاه مطبوعات، عنوان کرد: محل غرفه های مطبوعات و نشریات دانشگاهی در بیستمین نمایشگاه مطبوعات و خبرگزاری ها در جای خوبی قرار نگرفته بود.فکر میکنم ایشان جزو معدود افرادی(البته به جز مسئولین وزارتین علوم و بهداشت) بودند که به غرفه های دانشجویی توجه کرده بودند که امیدواریم که به دلیل نزدیکی به انتخابات نبوده باشد ما که نمی دانیم ولی اگر هم بوده باز هم دستشان درد نکند و ممنون از توجهشان.

اما سوالی که برای من مطرح بود این بود که چرا اغلب شخصیت ها فقط از خبرگزاری های معروف و نامی بازدید میکنند و غالبا هم سراغ خبرگزاری مرتبط با حذب و گروه خودشان می روند ؟سوالی که جوابش را اینگونه تعبیر کردیم که نمایشگاه مطبوعات مثل عید دیدنی کردن است که هر کس به منزل اقوام خودش میرود.

نکته ی قابل توجه دیگر این بود که امسال حضور خبری رسانه های خارجی در نمایشگاه بسیار کم رنگ بود. به طوری که میتوان گفت عنوان های خارجی تنها محدود میشدند به هفت عنوان (تهران تایمز، بنیاد اندیشه های نو، نمو، تینیجر اند لدر، صفحه ی اول، ایران فرانت پیج و موسسه ی مطبوعاتی نشرآوران)که توفیق حضور در مهم ترین رویداد رسانه ای را داشتند.

بازار کارگاه های آموزشی هم داغ بود بر اساس خبری که در سایت خبر آن لاین منتشر شده: به گزارش ستاد اطلاع رسانی بیستمین نمایشگاه مطبوعات، کارگاه‌های آموزشی این دفتر شامل آشنایی با فتوژورنالیسم ایران و جهان، کاربرد گرافیک خبری و اطلاع رسان در مطبوعات، چگونه یک گزارش داغ مطبوعاتی بنویسیم، روزنامه‌نگاری سایبر از سخت خبر تا رسانه‌های اجتماعی، مدیریت پورتال‌ها و وب سایت‌های اطلاع رسان، کارکرد بنگاه‌های رسانه ای در نشریات محلی است که هر روز از ساعت ۱۰/۳۰ تا ۱۲ با حضور استادان مطرح این حوزه برگزار می‌شود.

همچنین، ۶ نشست تخصصی با عناوین آموزش و پژوهش در حرفه روزنامه‌نگاری، الزامات ضروری در قانون مطبوعات، تکنولوژی نوین رسانه‌ای و نسل‌های بعدی رسانه، جایگاه نظام صنفی در رسانه‌های ایران، بررسی مشکلات نشریات محلی و جایگاه مطبوعات در اقتصاد مقاومتی نیز همه روزه از ساعت ۱۴ تا ۱۶ با حضور متخصصان و استادان حوزه رسانه و

مدیران مسئول نشریات برگزار شد. که بنده به دلیل اشتغال به تحصیل توفیق حضور در هیچ یک از آنها را نداشتم .
هم چنین درحاشیه ی نمایشگاه به گزارش سایت مهر جشن تولد ریاست جموری برگزار شد: در این مراسم که به همت خبرگزاری برنا و در محل غرفه این خبرگزاری برگزار شد یک روحانی جوان به نام عبدالمجید قوامی شعر کوتاه زیر را که هر مصرع آن با یک حرف از نام خانوادگی رئیس جمهور شروع شده بود، سرود:

ر روحانی من برادر حسن و وفا
و واله به خدا و دین و معیار هدا
ح حلم حسنی نصیحت اش بهر خدا
ا ایمان ز تو و حکم و علم والا
ن نامت چون حسن به حُسن مشهور و ولا
ی یاری بکنی رهبری ات با تقوا
.

در پایان این مراسم کوتاه و مختصر، حاضران در غرفه این خبرگزاری، شیرینی تولد رئیس جمهور را میل کردند.
براساس این گزارش حسن روحانی در ۲۱ آبان ۱۳۲۷ متولد شده ولی تاریخ صدور شناسنامه او ۹ دی ماه همان سال است.
ما که در این جشن تولد هم توفیق حضور نداشتیم و با گشتی که در این سایت و آن سایت زدیم این خبرجالب را پیدا کردیم ولی باور بفرمایید که شعر یاد شده خواندنش بس دشوار است کاش کمی بیشتر وزن و آهنگ داشت.
چهره هایی که ما در این بازدید شش ساعته در روز پنج شنبه موفق به دیدنشان شدیم عبارتند از جنابان:آقای نهاوندیان آقای جنتی وزیر فرهنگ آقای عارف آقای خرازی آقای سردار نقدی آقای پور محمدی و در نهایت هم خانم فائزه هاشمی که برای بازدید از غرفه ی دانشگاه آزاد به سمت غرفه های دانشجویی آمده بودند.
البته اتفاق جالبی هم در این بین رخ داد ما که در حال سیر و سیاحت به طور آماتور در جشنواره بودیم جلوی غرفه ی ایرنا ایستاده بودیم که آقای عارف قصد بازدید از این غرفه را داشتند و ما که یک دوربین کامپکت و خیلی کوچک در دست داشتیم را با خبرنگاران حرفه ای غرفه ی ایرنا اشتباه گرفته و احوالپرسی گرمی فرمودند که هنوز هم ازآن محضوضیم.
دم دم های غروب بود که قصد عزیمت به منزل را داشتیم که ناگاه دو تن از هنرمندان عزیز کشورمان را زیارت کردیم و آنها را برای بازدید از غرفه دعوت نمودیم آقایان فرشید فهیم (مجری)وکریم قربانی(بازیگر) که آقای قربانی هم مثل همیشه با شور و هیجانی که داشتند فضای غرفه ی ما را عوض کردند . راستی بین خودمان بماند اینجا بود که ما حدس زدیم که شایدبایستی مهمانان نمایشگاه را خودمان دعوت میکردیم که هنوز هم که هنوز است ما سر در گمیم که ما باید دعوت کنیم یا مورد بازدید واقع شویم.
نمایشگاه تمام شد و باز هم مثل همیشه غرفه ی دانشگاه الزهرا افتخار آفرید و غرفه ی برتر شد که همین جا صمیمانه به سرکار خانم زهرا وزیری کارشناس نشریات دانشگاه الزهرا تبریک می گوییم.

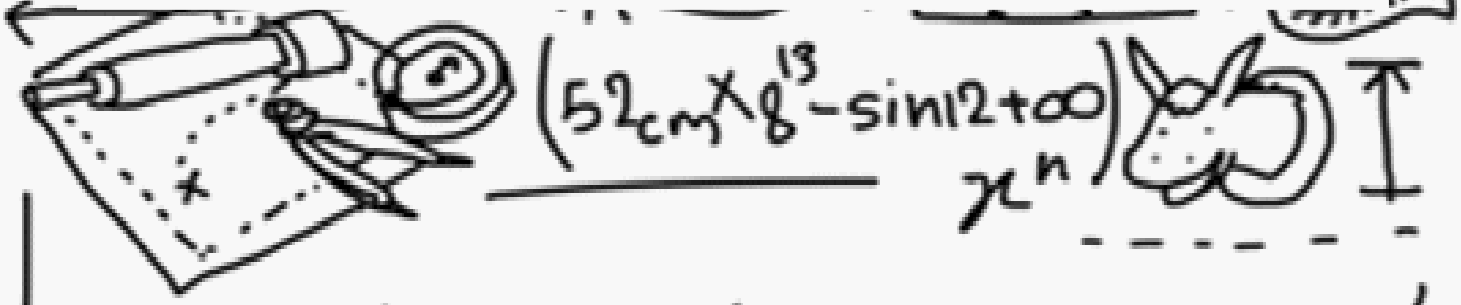
نویسنده: مهسا زمان – با تشکر از مهدیه ابراهیمی

● یک پیشنهاد :

نویسنده: رویا کشاورز

این بار میخوام یه کتاب بهتون معرفی کنم؛اسمش اندازه گیری دنیا هستش. نویسنده کتاب دانیل کلمان هستش .
این درسته که در کتاب های تاریخی چنین داستانی نیومده؛ اما در رمان دانیل کلمان نتیجه ی ملاقات سال ۱۸۲۸ بین دو نابغه شگفت انگیز و غیر عادی ؛ خواندنی است.
یکی جغرافی دان و کاشف سرزمین های دور؛ الکساندر فون هومبولت است و دیگری ریاضی دان سرشناس کارل فدریک گاووس. نتیجه این دیدار سفری است پر ماجرا برای اندازه گیری دنیا.

این کتاب پرفروش ترین رمان سه دهه ی اخیر ادبیات آلمان می باشد.
اندازه گیری دنیا خوانندگان و منتقدان را خنداند و به حیرت وا داشت.
نیویورک تایمز طنز خلاقانه و قصه پردازی دانیل کلمان را با دیوید پینچون نویسنده ی نابغه ی آمریکایی مقایسه کرد و گاردین آن را نمونه ای از یک شاهکار مدرن اروپایی خواند.



اندازه گیری دنیا

دانیل کلمان
ناتالی چوبینه