

## مشت نمونه خروار



محمد جواد لاریجانی

رئیس مرکز تحقیقات  
فیزیک نظری و ریاضیات

باسمه تعالی

در این شماره:

مشت نمونه خروار

خلاصه سخنرانی دکتر تجویدارزاده

شبکه در اخبار

رمزبندی پیامها

تازه‌های شبکه

آداب شبکه

اخباری از مرکز

آنچه گذشت

انتشارات مرکز

گزارشی از کتابخانه مرکز

برنامه‌های فصل

۱. توفیقات تحسین برانگیز دانش‌آموزان عزیز در المپیادهای علمی مسلم علامت توفیق سیستم آموزش قبل از دانشگاه کشور است؛ اما از همه مهمتر: نشان می‌دهد که ایران اسلامی صاحب گنجهای نهفته و بالقوه فکری و علمی است که مسابقات المپیاد فقط برخی از آنها را معین می‌کند - چه بسیارند ذهنهای قابل برای کاوشهای عمیق در علوم که معمولاً «بدامتحان» هستند لیکن در میدان فهم و تعمق و دقت و نوآوری پهلوان می‌باشند. مهم این است که باور کنیم: می‌توانیم!

۲. سؤال مهم و مسؤلیت اساسی این است که چگونه می‌توان افراد دانش‌طلب و بااستعداد را در امر دانش‌پژوهی یاری داد؟ چگونه می‌توان نقش علمی آنان را زنده نگه داشت و آنان را در رقابت حقیقی علمی وارد کرد؟ من متأسف خواهم بود اگر بشنوم برخی از عزیزان که در المپیادها افتخاراتی به دست آوردند احساس کنند دیگر در ایران نمی‌توانند درس بخوانند و حتماً باید به دانشگاه با نام و آوازه‌ای در خارج بروند و یا اینکه خدای ناکرده احساس کنند کار علمی آنان تمام شده است! این عزیزان باید بدانند، و وظیفه رسانه‌ها و شخصیت‌های علمی و فرهنگی این است که به آنها القاء کنند، که تازه کار اصلی که تعمق در علوم و رسیدن به افقهای جدید و نوآوری است برای آنها آغاز شده است.

۳. اکنون جانب دیگر قضیه را در نظر می‌گیریم: ایران زمین استعدادهای جوان و بسیار ممتازی دارد؛ پرورش این استعدادها و شکوفا کردن آنها چگونه است و چه نیازهایی دارد؟ به نظر من سه مورد زیر اساسی هستند:

اول. مهمترین عامل، این است که استادانی فداکار خود را وقف تربیت دانشجویان نمایند و با تمام وجود به این امر قیام نمایند. سیره مبارک و حسنه علمای سلف در این

سایر ملل رجوع معکوس را نشان می‌دهد: صاحبان صنایع برای مقاصد خود حاضر به سرمایه‌گذاری در پروژه‌های علمی می‌شوند! و دولت هم با ترفندهای مالیاتی مشوق آنان است. خلاصه کلام اینکه: در عین اذعان به تأثیر کاربردها و علایق تکنولوژیک در توسعه علوم و فنون، هرگز نباید فراموش کرد که معارف دارای یک ساختار طبیعی رشد نیز هستند. عالمان در امر تحقیق و شاگردپروری عمدتاً باید بر این طبیعت ذاتی علم اتکا کنند.

سوم. رسانه‌های کشور نیز می‌توانند دخیلی وثیق در ایجاد شوق علمی در جوانان و دانشمندان داشته باشند به شرط اینکه گرفتار دره «عوامی» نشوند! خیلی بد است که روزنامه‌ها و رادیو و تلویزیون بدون مشورت علمای کشور فرد یا کاری را یک کشف بزرگ یا مکتشف بزرگ اعلام کنند! جامعه علمی کشور می‌تواند به راحتی رسانه‌ها را در این زمینه از مشورت خود بهره‌مند کند.

والسلام.

زمینه باید احیا شود که آنان هرگز تربیت شاگرد را با صرف‌القاء چند درس اشتباه نمی‌کردند، بلکه محصول حیات علمی خود را در درجه اول در تربیت شاگردان می‌دیدند و سپس در القاء درس و یا نوشتن کتاب و رساله.

دوم، اتخاذ سیاستهای درست از سوی دولتها و اجرای مناسب آن سیاستهاست. مثلاً سرمایه‌گذاری در امر تحقیقات چه در دانشگاهها و چه در مراکز تحقیقاتی تصمیمی درست است، اما باید این امر با حساب و کتاب و به دور از عوام‌فریبی و شارلاتانی باشد؛ باید بر اساسی یک تصویر آینده‌نگرانه برای کشور و علم باشد که توسط اهل فن ترسیم شده است. در غیر این صورت، «تحقیقات» خود دکانی می‌شود که نه تنها مشوق تعشق علمی نخواهد بود بلکه مانع آن هم می‌تواند باشد. از سوی دیگر فرستادن علما به پشت در صاحبان صنایع برای گرفتن پروژه‌های تحقیقاتی امری سؤال‌برانگیز است. ظاهر کار این است که در این اقدام، هم مسائل صنعت پیشرفت می‌کند و هم کار علمی؛ اما مسأله به این سادگی نیست! این در شرایط امروز صنعت و جامعه علمی کشور می‌تواند به سرعت منجر به پایین آمدن سطح علمی کارها و کشتن علاقه مطالعه بسیاری از زمینه‌های اساسی در علوم بشود. تجربه

## خلاصه سخنرانی دکتر تحویلدارزاده

### نگاشتهای هارمونیک در خمینه‌های لورنتسی

نقض نیز که امکان بروز تکینه‌ها را اثبات کند یافت نشده. مسأله موجگاشت در ابعاد بالاتر،  $m \geq 3$ ، آب‌بحرانی است. در این ابعاد قضایایی در باره بروز تکینه‌ها در مدت زمان باپایان برای جواب مسأله کوشی با داده‌های آغازین کاملاً هموار موجود است و به‌طور یقین هیچ گزاره کلی در باب همواری سراسری جوابها در ابعاد بالا نمی‌تواند صحیح باشد.

در بخش میانی سخنرانی به معرفی چند قضیه در خصوص همواری سراسری جواب مسأله کوشی برای موجگاشتها در بعد  $m = 2$  می‌پردازیم. نقطه مشترک مابین این قضایا آن است که در همه آنها فرض می‌شود که داده‌های آغازین دارای نوعی تقارن هستند. این فرضهای تقارن (یکسان‌وردی و ناوردایی) نقشی کلیدی در اثبات قضایای مورد بحث بازی می‌کنند و تاکنون راهی برای حذف آنها و اثبات قضایای مشابهی برای موجگاشتها غیرمتقارن یافت نشده است.

در بخش پایانی سخنرانی قضیه بروز تکینه‌های خودشبه در بعد  $m = 3$  را بیان و به اثبات آن اشاره می‌کنیم و سپس مختصری راجع به مسأله حل‌نشده متناظر با این قضیه در بعد  $m = 4$  و برنامه سخنران برای حل آن بحث می‌نماییم.

موجگاشتها یا نگاشتهای هارمونیک خمینه‌های لورنتسی که نزد فیزیکدانان به سیگنال‌مدل شهرت دارند از زمره ساده‌ترین و طبیعی‌ترین میدانهای غیرخطی هندسی قابل تعریف روی فضا-زمان می‌باشند که در سالهای اخیر مورد توجه ریاضیدانان قرار گرفته‌اند. در این سخنرانی ابتدا قوانین پایستگی‌ای که از صفر بودن دیورژانس تانسور انرژی تکانه موجگاشت ناشی می‌شود و برآوردهای انرژی متوجه از آنها را معرفی کرده سپس به بررسی مسأله همواری سراسری کوشی برای موجگاشتها می‌پردازیم. با استفاده از استدلالی مقیاسی می‌توان دید که  $m$ ، بعد فضایی خمینه لورنتسی‌ای که دامنه موجگاشت است، نقش تعیین‌کننده‌ای در این مسأله بازی می‌کند: مسأله موجگاشت را در بعد  $m = 1$  زیر بحرانی می‌خوانیم، و دیده می‌شود که مسأله کوشی در این بعد، بدون وجود هیچ‌گونه قید و شرطی روی بزرگی داده‌های هموار آغازین، همیشه دارای جوابی یگانه و سراسر هموار است. بعد  $m = 2$  برای موجگاشتها بعد بحرانی است. در این بعد مسأله همواری سراسری جواب مسأله کوشی در حالت کلی هنوز حل نشده است در حالی که هنوز مثالی

## شبکه در اخبار

تهیه و تنظیم: سعید وحید

### رمزبندی پیامها

پیامها و پرونده‌هایی که روی شبکه اینترنت فرستاده می‌شود برای رسیدن به مقصد نهایی باید از چندین ایستگاه بینابینی عبور کند. تمام ایستگاههای شبکه سطح امنیتی یکسانی ندارند: برخی از آنها کاملاً حفاظت شده هستند و نفوذ به آنها به‌سادگی امکان‌پذیر نیست، ولی تعدادی دیگر ممکن است چنین نباشند، یعنی افراد با مهارت که دارای سوءنیت یا مقاصد خرابکارانه باشند می‌توانند با کمی تلاش به چنین سیستم‌هایی نفوذ کنند و به اطلاعات موجود در آنها، از جمله پیامها و پرونده‌هایی که روی شبکه رد و بدل می‌شود، دسترسی یابند.

برای رفع این مشکل، روشهای مختلفی ابداع شده است که یکی از آنها استفاده از یک کامپیوتر واسط بین کامپیوتر اصلی و شبکه اینترنت است. این کامپیوترها که به دیوار آتش (firewall) موسوم‌اند حفاظت از کامپیوتر اصلی در مقابل نفوذ افراد غیرمجاز را به عهده می‌گیرند و در واقع چنین نفوذی را غیرممکن می‌سازند. به‌کارگیری دیوار آتش هزینه زیادی به همراه دارد از این رو تمام ایستگاههای شبکه از آن استفاده نمی‌کنند. پس تا زمانی که تمام ایستگاههای شبکه به چنین سیستمی مجهز شوند باید به دنبال راه دیگری بود. روشی که از دیرباز برای حفاظت پیامها و نامه‌ها به‌کار می‌رفته رمزبندی (encryption) است. در این روش، پیام با استفاده از رمزی که نویسنده و همچنین گیرنده پیام به آن دسترسی دارند تهیه می‌شود تا از دسترسی سایرین به محتوای آن جلوگیری شود. مشابه این روش در شبکه اینترنت نیز ابداع شده است. استفاده از رمزبندی کامپیوتری، صرف‌نظر از کاربردهایی که در مکاتبات جدی ممکن است داشته باشد، سبب آشنایی جامعه علمی کشور با شگردها و الگوریتمهای به‌کاررفته در این سیستم خواهد شد که خود بسیار مهم است.

سیستم رمزبندی رایج در اینترنت 'PGP' خوانده می‌شود که مخفف کلمات pretty good privacy است. این سیستم در سال ۱۹۹۱ توسط فیلیپ زیرمن ابداع شد. با استفاده از PGP می‌توان پیامها را به‌گونه‌ای رمزبندی کرد که فقط کسانی که نویسنده پیام مد نظر دارد بتوانند آن را بخوانند. علاوه بر این، PGP امکان می‌دهد تا نویسنده، پیام خود را امضا کند. با استفاده از این امضای الکترونیک، گیرنده می‌تواند مطمئن باشد پیامی را که دریافت کرده واقعاً از جانب نویسنده است و کسی در بین راه آن را دستکاری نکرده است. روش رمزبندی PGP محبوبیت فراوانی یافته است که دلایل آن را می‌توان چنین برشمرد:

- بهترین الگوریتمهای رمزبندی (IDEA, RSA, MD5) در آن به‌کار رفته است.
- این الگوریتمها در نرم‌افزاری گنجانده شده‌اند که روی اکثر سیستم‌عامل‌ها

اجرا می‌شود و استفاده از آن نیز آسان است.

- این نرم‌افزار، مستندات همراه آن و حتی متن برنامه (source code) به‌رایگان در اختیار همگان قرار دارد.

در نرم‌افزار PGP برای رمزبندی اطلاعات از کلیدهایی استفاده می‌شود که با استفاده از یک مولد اعداد تصادفی (random number generator) درست می‌شوند. این مولد از جنبه رمزبندی داده‌ها بسیار قدرتمند است. هسته (seed) های مورد نیاز برای تولید اعداد تصادفی روی پرونده‌ای ذخیره می‌شود. هنگام تولید این پرونده از اعداد کاملاً تصادفی، مانند فاصله زمانی بین فشردن کلیدها توسط کاربر، استفاده می‌شود. هر بار که این مولد اجرا می‌شود پرونده حاوی هسته‌ها را با استفاده از منابع کاملاً تصادفی، مانند ساعت اجرا، به‌نگام کرده هسته‌های جدیدی وارد آن می‌سازد.

الگوریتمهای به‌کارگرفته‌شده در PGP برای رمزبندی اطلاعات ترکیبی از IDEA و RSA است، به این ترتیب که برای رمزبندی کلیدها از الگوریتم RSA، و برای رمزبندی متن اصلی از الگوریتم IDEA - به خاطر سرعت زیاد آن - استفاده می‌شود. اندازه بلوک‌های متن معمولی (plaintext) و متن رمزبندی‌شده (ciphertext) در الگوریتم IDEA ۶۴ بیت است و در آن از کلیدهای ۱۲۸ بیتی استفاده می‌شود. این الگوریتم بر اساس مفاهیمی در نظریه گروه‌ها بنا شده است. الگوریتم IDEA در سال ۱۹۹۰ در دانشگاه ETH زوریخ در سوئیس ارائه شد و از آن زمان تلاشهای زیادی برای شکستن رمزبندی شده با IDEA در محافل دانشگاهی و نظامی در سراسر دنیا انجام گرفته که همه ناموفق بوده‌اند و این امر سبب شده تا اعتماد نسبت به این روش بیشتر شود. قبل از آن برای امتحان الگوریتمی موسوم به DES، یکی از پژوهشگران توانسته بود مداری را طراحی و آزمایش کند که می‌توانست در هر ثانیه ۵۰ میلیون کلید را حدس بزند. به گفته او ساخت این مدار با هزینه ۱۰ دلار امکان‌پذیر بود و می‌شد با صرف یک میلیون دلار کامپیوتری ساخت که ۵۷,۰۰۰ عدد از این مدارها را در خود جای دهد. این کامپیوتر حداکثر در مدت ۷ ساعت (به‌طور متوسط ۳٫۵ ساعت) می‌توانست رمزهای DES را بگشاید. الگوریتم IDEA قوی‌تر از DES است و تاکنون روشی مشابه روش فوق برای شکستن رمزهای آن ارائه نشده است.

نرم‌افزار PGP قبل از رمزبندی متن، آن را فشرده (compress) می‌سازد، زیرا فشرده‌سازی بعد از رمزبندی عملی نیست. مزیت فشرده‌سازی در این است که مدت زمان ارسال اطلاعات روی خطوط ارتباطی کوتاهتر می‌شود و اطلاعات فشرده جای کمتری را روی دیسک اشغال می‌کنند. مهمتر از همه اینکه فشرده‌سازی ضریب اطمینان رمزبندی را بیشتر می‌کند. بسیاری از روشهایی که برای شکستن رمز به‌کار می‌روند از افزونگی (redundancy) های موجود در متن اصلی برای کشف رمز استفاده می‌کنند؛ ولی وقتی که اطلاعات فشرده شوند چنین افزونگیهایی در آنها وجود نخواهد داشت. روش فشرده‌سازی

نرم افزار PGP برای کاربردهای غیرتجاری رایگان است و روی اکثر سیستم عامل ها، مانند یونیکس، DOS، VAX، و غیره، می توان آن را اجرا کرد. اگرچه این نرم افزار یک راهنمای ۷۵ صفحه ای دارد ولی استفاده از آن ساده است. نسخه مخصوص سیستم عامل DOS = نرم افزار PGP در کامپیوتر «زاگرس» مرکز تحقیقات موجود است و با روش انتقال پرونده (ftp) از نشانی [zagros.ipm.ac.ir](mailto:zagros.ipm.ac.ir) می توان آن را دریافت کرد. این نرم افزار در کشور (directory) [pub/msdos/PGP/](http://pub/msdos/PGP/) و در پرونده [pgp262i.zip](http://pub/msdos/PGP/pgp262i.zip) قرار دارد.

نخستین کاری که پس از نصب برنامه و مطالعه پرونده راهنما باید انجام دهید، تولید کلید شخصی و همگانی با استفاده از دستور `pgp -kg` است. اجرای این دستورات سبب می شود تا دو کلید و دو جاکلیدی (key-ring) درست شود. جاکلیدی همگانی ای که به این ترتیب ایجاد می شود محلی است که کلید همگانی دوستان و همکاران خود را در آن قرار خواهید داد. پس از آن باید نسخه ای از کلید همگانی خود را تهیه و برای دوستان و همکارانتان ارسال کنید. این کار را می توان با استفاده از دستور `pgp -kxa` انجام داد. برای مثال کلید همگانی نویسنده در انتهای مقاله آمده است.

وقتی دیگران کلید همگانی شما را دریافت می کنند باید آن را با دستور `ka` - به جاکلیدی خود اضافه کنند. پس از آنکه کلید همگانی شخصی را به جاکلیدی خود اضافه کردید می توانید برای او پیام رمزبندی شده بفرستید و همچنین امضای الکترونیک او در زیر نامه ها را تأیید کنید. فرض کنید کلید همگانی شخصی به نام «علی» را با دستور فوق به جاکلیدی خود اضافه کرده اید و اکنون می خواهید نامه ای را با استفاده از PGP رمزبندی کرده برای او بفرستید. اگر این نامه در پرونده ای به نام `letter.doc` باشد با اجرای دستور زیر می توان به هدف فوق رسید:

```
pgp -ea letter.doc
```

پرونده ای را که در نتیجه اجرای این دستور ایجاد می شود می توان با پست الکترونیک برای علی فرستاد و او نیز می تواند آن را با استفاده از کلید شخصی خود رمزگشایی کرده بخواند.

اطلاعات بیشتر در مورد PGP از جمله نسخه های مخصوص سیستم عامل های گوناگون و متن برنامه را می توان از نشانی <http://www.ifi.uio.no/taalesc/PGP/home.html> به دست آورد.

که در PGP استفاده می شود 'ZIP' نام دارد و همان روشی است که در نسخه ۲/۰ برنامه PKZIP نیز به کار رفته است. علت انتخاب ZIP این بوده است که جزئیات و متن کامل برنامه به رایگان در اختیار همگان قرار دارد و علاوه بر این از سرعت اجرا و ضریب فشردگی خوبی برخوردار است.

برای تولید امضای الکترونیک، PGP خلاصه ای از پیام (message digest) را رمزبندی کرده در انتهای متن قرار می دهد. خلاصه پیام، یک بلوک ۱۲۸ بیتی فشرده شده و «تلخیص شده» از آن پیام است و شبیه مجموع مقابله ای (checksum) عمل می کند. (برای مثال، رقم سمت راست در ISBN کتابها مجموع مقابله ای است و برای کنترل درستی بقیه ارقام از آن استفاده می شود). خلاصه پیام را می توان به عنوان اثر انگشت پیام نیز در نظر گرفت، یعنی هر پیام اثر انگشت منحصر به فرد خود را دارد و چنانچه متن پیام قبل از رسیدن به دست گیرنده اصلی دستکاری شود، چون تطابق بین متن و امضا (اثر انگشت) از بین می رود گیرنده می تواند متوجه ایجاد تغییر شود. امضا فقط حاوی خلاصه پیام نیست چرا که الگوریتمهای تولید خلاصه پیام در دسترس همگان قرار دارد، و بنابراین سارق اطلاعات به راحتی می تواند در متن پیام تغییر دهد و با تولید خلاصه پیام جدید، آن را دوباره برای گیرنده اصلی ارسال کند. برای امضای متن، باید کلمه رمز امضاکننده نیز ارائه شود؛ بنابراین امکان ایجاد تغییر و قرار دادن امضای جدید منتفی می شود. در PGP از یک تابع درهم سازی یک سویه (one way hash function) برای تولید خلاصه پیام استفاده می شود. بنابراین، از دیدگاه محاسباتی محال است کسی بتواند پیام اصلی را با پیام دیگری عوض کند که امضای هر دو یکسان باشد. الگوریتمی که در PGP برای تولید خلاصه پیام به کار می رود 'MD5' نام دارد.

روش استفاده از PGP به این شکل است که هر استفاده کننده دو کلید دارد: کلید شخصی (secret key) و کلید همگانی (public key). کلید شخصی از دسترس دیگران دور نگه داشته می شود ولی کلید همگانی در اختیار کسانی که با نویسنده پیام مکاتبه دارند گذاشته می شود. برای مثال، اگر دوستانتان بخواهند برای شما نامه ای بفرستند، قبل از ارسال آن را با کلید همگانی شما رمزبندی می کنند و فقط کلید شخصی شماست که می تواند رمز آن پیام را بگشاید. اگر بخواهید پیامی را امضا کنید این کار را با استفاده از کلید شخصی خود انجام می دهید و دوستانتان می توانند با کمک کلید همگانی شما اطمینان پیدا کنند که نویسنده واقعی آن پیام شما بوده اید.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: 2.6.2i
```

```
mQBtAzAM9u0AAAEDAMh+P9Y0aVbjaKPYBEW OnXM47wQ0eQTZsns4TyFVp2LTmcTr
```

```
qzOedGs7LEgyRb3DMnzJz4Mzo539fLrXVnzG5km+ LZjgp8nE3GxFC7wQ6XQLuXMN
```

```
Uqx8jkmJf1c6qhFqfQAFEBqBU2F1ZWQgVmFoaWQ gPHZhaG1kQGdwZy5jb20+
```

```
=00DV
```

```
-----END PGP PUBLIC KEY BLOCK-----
```

## تازه‌های شبکه

### گسترش شبکه

در سه ماهه اول سال ۱۳۷۴ ارتباط وزارت فرهنگ و آموزش عالی-ساختمان شماره ۲ (از طریق ساختمان نیاوران مرکز تحقیقات)، وزارت بهداشت، درمان و آموزش پزشکی (از طریق دانشگاه تربیت مدرس)، مرکز مطالعات مدیریت و بهره‌وری ایران (از طریق ساختمان اختیاریه)، و مرکز پژوهش‌های مجلس شورای اسلامی (از طریق ساختمان اختیاریه) با شبکه برقرار شد.

دانشگاهها و مراکز دیگری که اتصال آنها به شبکه در آستانه راه‌اندازی است عبارت‌اند از: مرکز مطالعات وزارت امور خارجه، دانشگاه علوم پزشکی ایران، دانشگاه علوم پزشکی تهران، و دانشگاه خواجه نصیرالدین طوسی.

آخرین وضعیت اتصالات در شکل صفحه بعد نشان داده است.

### برگزاری سمینار ۲ روزه سیستم‌های باز گسترده

سمینار ۲ روزه سیستم‌های باز گسترده در ۳۰ و ۳۱ اردیبهشت ماه سال جاری در مرکز تحقیقات فیزیک نظری و ریاضیات (ساختمان اختیاریه) برگزار گردید. سخنرانان این سمینار دانشجویان کارشناسی ارشد دانشگاه آزاد اسلامی (واحد جنوب) بودند و در چهار زمینه سیستم‌های باز و مدیریت آنها، تکنولوژی اینترنت و جغرافیای آن، محیط‌های توسعه سیستم‌های باز، و شبکه‌های سریع اطلاعاتی مجموعاً بیست سخنرانی ایراد شد. این سمینار با استقبال بسیار خوبی روبه‌رو گردید.

### برگزاری دوره‌های آموزشی

یک دوره آموزش نظری و سه کارگاه آموزشی در مورد مفاهیم و خدمات شبکه در خرداد ماه ۷۴ از طرف واحد کامپیوتر مرکز تحقیقات برگزار شد. این دوره‌های آموزشی عبارت بودند از:

دوره آموزشی یک‌روزه آشنایی با خدمات شبکه در تاریخ ۷۴/۳/۲۲، کارگاه عملی ftp و Archie در تاریخ ۷۴/۳/۲۴، کارگاه عملی gopher در تاریخ ۷۴/۳/۲۷، کارگاه عملی WWW در تاریخ ۷۴/۳/۲۹.

این دوره‌های آموزشی، مخصوصاً کارگاه‌های عملی خدمات شبکه، با استقبال بسیار گسترده‌ای از سوی کاربران شبکه روبرو شد. این دوره‌های آموزشی هر ماه توسط واحد کامپیوتر مرکز ارائه خواهد شد.

### راه‌اندازی خدمتکار WWW

نرم‌افزار خدمتکار WWW (WWW server) بر روی سیستم کامپیوتر SUN مرکز تحقیقات نصب گردید و استفاده از آن برای کاربران شبکه فراهم شد. سرویس WWW یکی از سرویس‌های جدید و در عین حال محبوبترین سرویس در شبکه اینترنت است و از ویژگی‌های آن، امکانات چندرسانه‌ای (multimedia) مانند تصاویر رنگی، صدا، و حتی تصاویر متحرک (انیمیشن) است.

بر طبق آمارهای موجود، کاربران سرویس WWW هر چهل روز یک‌بار، دوبرابر می‌شوند.

### ثبت نشانیهای اینترنت در ایران

مرکز تحقیقات فیزیک نظری و ریاضیات رسماً به‌عنوان مرکز ثبت محلی نشانیهای اینترنت (local IP registry) در ایران پذیرفته شد. بدین ترتیب، کلیه دانشگاه‌ها و مراکزی که در داخل ایران تقاضای دریافت نشانیهای IP دارند باید درخواست خود را در اختیار مرکز قرار دهند تا از این طریق مطابق مقررات شبکه اینترنت اقدام گردد.

از این پس درخواستهای دانشگاه‌ها و مراکز تحقیقاتی که در شبکه قرار می‌گیرند برای دریافت نشانی IP با سرعت به مراتب بیشتری از سابق پردازش می‌گردد و نشانیهای معتبر جهانی از سوی مرکز در اختیار آنان قرار داده می‌شود.

### خدمتکار gopher مرکز در جداول بین‌المللی

خدمتکار gopher مرکز رسماً در بین خدمتکارهای gopher بین‌المللی به ثبت رسید. به این ترتیب، نام خدمتکار gopher مرکز در کلیه جداول بین‌المللی درج گردید و اطلاعات آن برای تمام کاربران شبکه اینترنت در سراسر جهان قابل دستیابی شد. شایان ذکر است که در منطقه خاورمیانه به جز خدمتکار gopher مرکز تحقیقات، ۱۲ خدمتکار gopher از اسرائیل، یک خدمتکار gopher از مصر، و یک خدمتکار gopher از تونس به ثبت رسیده‌اند.

### اتصال با دانشگاه گیلان از طریق VSAT

با نصب آنتنهای ماهواره‌ای مربوط، ارتباط دانشگاه گیلان با شبکه برقرار گردید. هم‌اکنون کارشناسان مرکز تحقیقات و دانشگاه با کمک مهندسان شرکت مخابرات سرگرم آزمایش پروتکل‌های مختلف موجود بر روی سیستم HUB مخابرات و ارزیابی سرعت انتقال داده‌ها بین دو شبکه می‌باشند.

### جلسات کمیته شبکه کشور

کمیته شبکه کشور که به منظور همکاری و هماهنگی بیشتر برای گسترش شبکه و راهبری فعالیتهای اجرایی از نمایندگان و افراد رابط دانشگاه‌ها و مراکز تحقیقاتی متصل به شبکه تشکیل گردیده است، جلسات منظم خود را به‌طور ماهیانه برگزار می‌کند.

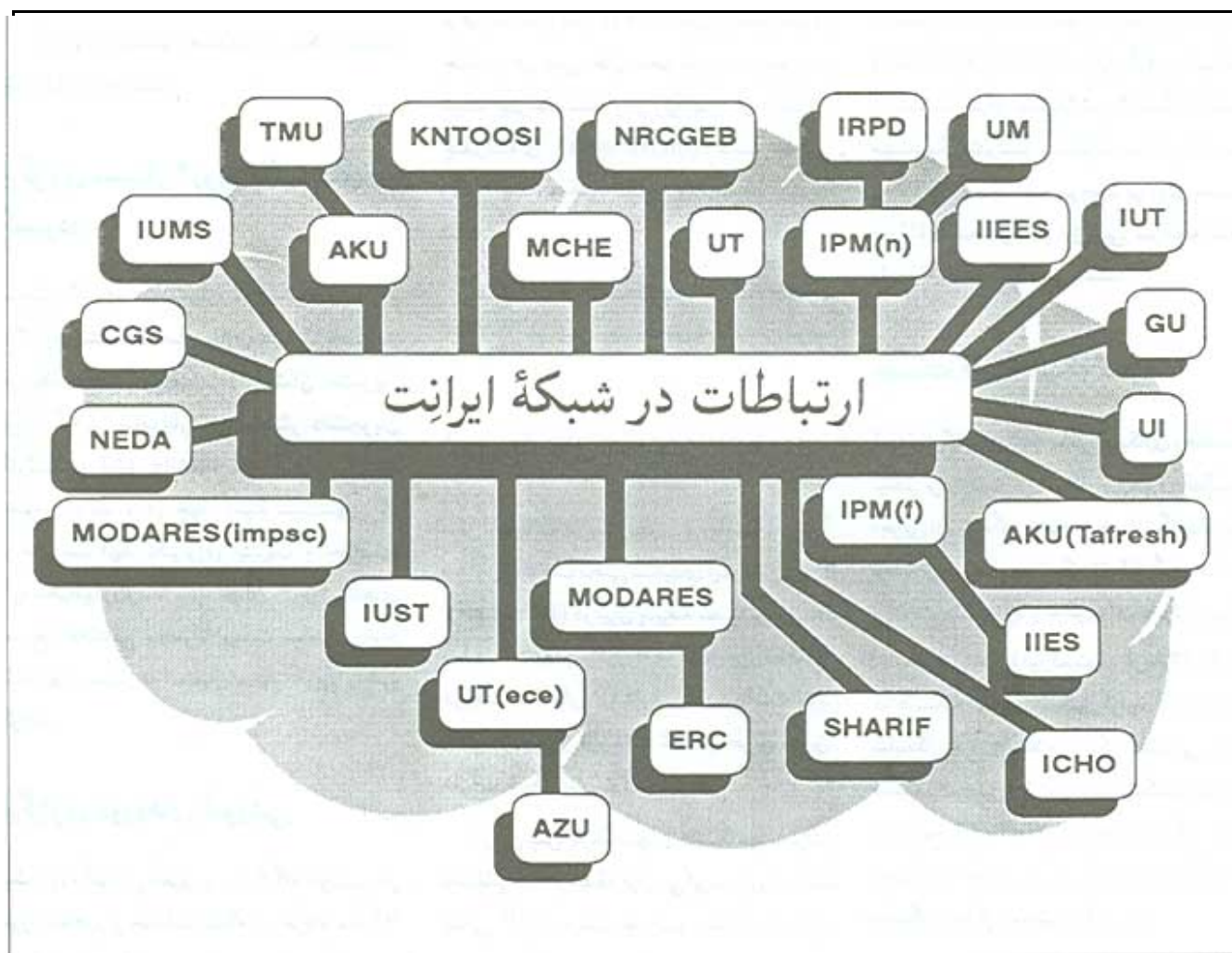
هفتمین جلسه این کمیته در تاریخ ۷۴/۲/۱۳ در دانشگاه اصفهان تشکیل گردید. در این جلسه نمایندگان ۱۱ دانشگاه و مرکز تحقیقاتی حضور داشتند. همچنین هشتمین نشست کمیته شبکه نیز در تاریخ ۷۴/۳/۲۴ در محل دانشگاه خواجه نصیرالدین طوسی و در حضور نمایندگان ۲۲ دانشگاه و مرکز پژوهشی برگزار شد.

از اهم موارد دستور جلسه این دو نشست می‌توان به این موارد اشاره کرد:



- گزارشی از گسترش شبکه شامل گروههای جدید
- گزارشی در مورد پیشرفتهای به عمل آمده در زمینه خدمات شبکه در کشور
- گزارشی درباره دفتر شبکه اطلاعات علمی نیروهای متخصص ایرانی مقیم داخل و خارج از کشور توسط دکتر منصور معین زاده مشاور وزیر فرهنگ و آموزش عالی
- گزارشی در مورد وضعیت شبکه و نحوه سرویس دهی به کاربران در دانشگاههای اصفهان و خواجه نصیرالدین طوسی
- بررسی امکان برگزاری کنفرانس سالانه ای تحت عنوان «خدمات شبکه» از سوی کمیته
- گزارشی از فعالیتهای انجام شده در کمیته شبکه وزارت فرهنگ و آموزش عالی
- گزارشی در مورد امکان سنجی طراحی شبکه آکادمیک کشور
- گزارشی در مورد امکان استفاده از پست الکترونیک فارسی
- نهمین جلسه کمیته شبکه در تاریخ ۷۴/۵/۱۱ در دانشگاه صنعتی شریف برگزار خواهد شد.

### شبکه ایران



## آداب شبکه (Netiquette)

### امنیت استفاده از کامپیوتر

اکثر کامپیوترهایی که به شبکه متصل هستند جزو سیستمهای چندکاربره (multi-user) به شمار می آیند و در چنین سیستمهایی برای اثبات هویت کاربران مجاز و جلوگیری از دسترسی افراد غیرمجاز به سیستم روشهای گوناگونی به کار گرفته می شود. یکی از این روشها استفاده از گذرواژه (password) است. گذرواژه کلمه ای است که فقط کاربر مجاز باید از آن اطلاع داشته باشد، و اگر این کلمه به دست اشخاص غیرمجاز بیفتد ممکن است وارد سیستم شده خسارتهای جبران ناپذیری به بار بیاورند.

در بعضی از سیستمها تا سه بار می توان گذرواژه را وارد کرد و چنانچه در هیچ یک از آن سه بار گذرواژه معتبر داده نشود سیستم امکان دسترسی مجدد را از کاربر سلب می کند. گذرواژه و نام کاربر (user name) در حکم کلیدهای ورود به سیستم هستند. هر کاربر، گذرواژه و نام کاربر

مخصوص خود را دارد که در ترکیب با یکدیگر امکان کار با سیستم را فراهم می آورند. سیستم و همچنین سایر کاربران، شما را با نام کاربر خودتان می شناسند. گذرواژه ترکیبی است از حروف الفبا، ارقام، و نویسه های ویژه که به منزله کلید عمل می کند. معمولاً برای اینکه بقیه نتوانند گذرواژه شما را ببینند هنگام تایپ آن، چیزی روی صفحه دیده نمی شود.

برای اینکه دیگران به راحتی نتوانند گذرواژه شما را حدس بزنند و به طور غیرمجاز وارد سیستم شوند بهتر است در گذرواژه انتخابی علاوه بر حروف الفبا از ارقام و نویسه های ویژه (مانند <، \$ و #) نیز استفاده کنید. چند نمونه از گذرواژه های خوب در زیر آمده است:

\*6burn0\*

+stol8=%

a\$gud<y

iaa77&r

88ber5@

سعی کنید هر از چند گاهی گذرواژه خود را عوض کنید. بعضی از سیستمها به طور خودکار در

فواصل زمانی معینی کاربران را وادار می کنند تا این کار را انجام دهند. هرگز گذرواژه خود را جایی ننویسید و آن را در اختیار دیگران قرار ندهید. اگر روی چند کامپیوتر نام کاربر دارید برای هر کدام، از گذرواژه های متفاوت استفاده کنید. سعی کنید در انتخاب گذرواژه از موارد زیر استفاده نکنید:

- اسم فرزندان یا همسر
- اسم خیابان محل سکونت یا شماره تلفن
- شماره شناسنامه
- رنگ یا مدل اتومبیل
- اسامی درختان، جانوران، رودخانه ها، شهرها، و استانها
- اسامی نقاط دیدنی شهر
- قهرمان فیلمها یا شخصیت های کارتونی

سرانجام اینکه اگر مدیریت سیستم با شماست سعی کنید در حضور دیگران به امنیت کامپیوتر خود مباحثات نکنید زیرا این کار، نفوذی (hacker)ها را که علاقه مند به ثابت کردن قابلیت های خویش هستند تحریک به مختل ساختن سیستم شما خواهد کرد.

## آیا می دانید که

- در ماه مارس ۱۹۹۵ (اسفند ۱۳۷۳/فروردین ۱۳۷۴) میزان افزایش ایستگاههای شبکه اینترنت در اروپا برابر با ۱۱ درصد بوده است.
- در اروپا ۳۰۰,۰۰۰ نفر مشترک خدمات شرکت کامپیوسرو هستند.
- در هر ساعت کاری در ماه مارس ۱۹۹۵، ۳۷ درخواست جدید برای ثبت نام دامنه جدید به مقامات مسؤل تحویل شده است.
- در نوز چهار برنامه تلویزیونی دارای تابلوی اعلانات در سرویس وب اینترنت هستند.
- در مصر چهار شرکت در زمینه ارائه خدمات دسترسی به اینترنت به عموم مشغول فعالیت هستند.
- یکی از استادان دانشگاه فرفیلد (Fairfield) در توصیف یک برنامه هوش مصنوعی که از راه خواندن مراسلات گروههای گفتگو (Usenet) انگلیسی یاد گرفته گفته است «لهجه شبکه ای وحشتناکی دارد.»



## اخباری از مرکز

- H. Brezis: *Analyse fonctionnelle, théorie et applications*, Masson, Paris, 1983.

### عبدالرضا تحویلدارزاده



عبدالرضا تحویلدارزاده، استادیار دانشگاه پرینستون که در تابستان امسال میهمان دانشکده علوم ریاضی دانشگاه صنعتی شریف است، به دعوت بخش ریاضی مرکز تحقیقات فیزیک نظری و ریاضیات دو سخنرانی در باره نگاهیهای هارمونیک در خمینه‌های لورنتسی ایراد نمود.

عبدالرضا (شادی) تحویلدارزاده پس از گرفتن لیسانس ریاضی در سال ۱۳۶۴ از دانشگاه صنعتی شریف، برای ادامه تحصیل به آمریکا رفت و در سال ۱۳۷۰ موفق به گرفتن دکتری ریاضی از انستیتوی علوم ریاضی کورانت در دانشگاه نیویورک شد. وی پایان‌نامه خود را با عنوان «نگاشتهای هارمونیک فضای مینکوفسکی» زیر نظر جلال شطح به رشته تحریر در آورده است. تحویلدارزاده پس از فراغت از تحصیل به مدت یک سال در انستیتوی مطالعات عالی در پرینستون و سپس دو سال در دانشکده ریاضی دانشگاه میشیگان در آن آربر به پژوهش و تدریس پرداخت و هم‌اکنون استادیار ریاضیات در دانشگاه پرینستون می‌باشد. تحقیقات وی در زمینه معادلات دیفرانسیل پاره‌ای غیرخطی و به‌طور اخص نظریه میدانهای لاگرانژی و مکانیک نسبیتی است.

2. nonlinearities with the *good sign*,
3. nonlinear perturbations,
4. quadratic and subquadratic nonlinearities in the gradient term,
5. monotone operators.

### III Semilinear elliptic equations (O. Kavian):

1. the superposition (or Nemytskiy) operators,
2. critical points on constraints and the Pohožaev identity,
3. semilinear problems in the whole space,
4. radial solutions and the *concentration-compactness* principle of P.-L. Lions,
5. the critical Sobolev exponent.

منابع کارگاه کتابهای ذیل می‌باشند:

- K. Yosida, *Functional Analysis*, Springer-Verlag, New York, 1980.
- N. Dunford and J.T. Schwartz, *Linear Operators* (3 volumes), Interscience, New York, 1988. Wiley
- L. Schwartz, *Méthodes Mathématiques de la Physique*, Hermann, Paris, 1961.

[یا مرجع کاملتر و کلاسیک

*Théorie des Distributions*, Hermann, Paris, 1966.

## دومین کارگاه آنالیز تابعی کاربرد و معادلات دیفرانسیل پاره‌ای

از ۲۱ الی ۲۹ تیر ماه امسال، دومین کارگاه آنالیز تابعی کاربردی و معادلات دیفرانسیل پاره‌ای توسط مرکز تحقیقات فیزیک نظری و ریاضیات و دانشکده علوم ریاضی دانشگاه صنعتی شریف در آن دانشگاه برگزار می‌شود. دکتر عطارد کاویان و پروفیسور فرانسوا مورا استادان برگزیده این کارگاه هستند و دفتر فرهنگی سفارت فرانسه در ایران در برگزاری کارگاه همکاری می‌کند.

کارگاه شامل ۱۶ جلسه ۹۰ دقیقه‌ای است که در سه بخش ارائه می‌شود. مفاد بخشها عبارتند از:

### I The common part:

1. some topics on distribution theory,
2. Sobolev spaces,
3. Lax-Milgram theorem,
4. minimization of convex functionals,
5. second-order elliptic boundary value problems (maximum principle, existence, uniqueness),
6. second-order elliptic operators (regularity of solutions, eigenvalues and spectrum).

### II Monotonicity and compactness in nonlinear problems (F. Murat):

1. bounded nonlinearities via Schauder and Brouwer theorems,



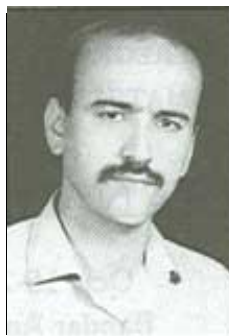
## فریدون شهیدی



فریدون شهیدی، استاد ریاضیات دانشگاه پردو، در نظریه اعداد شهرت جهانی دارد. او از معدود کسانی بود که نسخه اول اثبات وایلز از آخرین قضیه فرما را برای بررسی در اختیار داشت. شهیدی که صورت جدید اثبات را نیز مطالعه کرده است معتقد است که اکنون این اثبات کامل شده است، هرچند که اظهار می‌کند هنوز جزئیات بعضی قسمت‌ها را به دقت کافی بررسی نکرده است. سخنرانی

شهیدی در مرکز تحقیقات (تیر ۱۳۷۴) در این زمینه موقعیت مغتنمی برای جامعه ریاضی ایران است که جریان این رویداد مهم ریاضی را از زبان یکی از دست‌اندرکاران بشنود.

## مجتبی منیری



مجتبی منیری اخیراً پس از اخذ درجه دکتری خود در نظریه منطقی اعداد و مراجعت به ایران همکاری خود را با هسته تحقیقاتی منطق و علوم نظری کامپیوتر شروع کرده است.

مجتبی منیری پس از اخذ درجه فوق لیسانس از گروه ریاضی دانشگاه تهران در سال ۱۳۶۶، در سال ۱۳۶۷ به آمریکا رفت و در سال ۱۳۷۳ درجه دکتری خود را از دانشگاه مینه‌سوتا دریافت کرد. رساله ایشان تحت راهنمایی کارل پریگری و با عنوان «مدلهای استقرای باز و سریهای توانی تعمیم‌یافته» نگاشته شده است.

دکتر منیری در پاییز و زمستان ۷۳ در دانشگاه مینه‌سوتا استادیار بود.

## نظریه مجموعه‌های II

هسته تحقیقاتی منطق و علوم نظری کامپیوتر در نیمسال اول سال تحصیلی ۷۴-۷۵ درسی در نظریه مجموعه‌ها در دانشکده علوم ریاضی دانشگاه صنعتی شریف برگزار خواهد کرد. مدرس دکتر محمدجواد لاریجانی، و زمان درس شنبه‌ها ۸ تا ۱۰ و چهارشنبه‌ها ۱۳:۳۰ تا ۱۵:۳۰ خواهد بود.

دوره‌های درسی تابستانی هسته تحقیقاتی منطق و علوم نظری کامپیوتر (شروع: تیر ۱۳۷۴)			
موضوع	سخنران	زمان	مکان
مباحثی در نظریه مدلها	مسعود پورمهدیان	شنبه‌ها ۱۴-۱۵:۳۰	ساختمان نیاوران
مباحثی در نظریه بازگشت	فرزاد دیده‌ور	یکشنبه‌ها ۱۵-۱۶:۳۰	ساختمان نیاوران
منطق فلسفی II	حمید وحیددستجردی	سه‌شنبه‌ها ۱۴-۱۵:۳۰	ساختمان نیاوران
قضایای ناتمامیت گودل	صالح علی‌باری	چهارشنبه‌ها ۱۷-۱۵:۳۰	ساختمان نیاوران
استقرای باز	مجتبی منیری	پنجشنبه‌ها ۱۵-۱۳:۳۰	ساختمان نیاوران


سمینار هفتگی هسته تحقیقاتی جبر		
زمان	سخنران	عنوان
پنجشنبه ۷۴/۴/۱	کاظم خشیارمنش	بعد یکدست کسره‌های تعمیم‌یافته و قضیه گیبسن
پنجشنبه ۷۴/۴/۸	صمد حاج‌جباری	همبافتهای هیوز مدرج
پنجشنبه ۷۴/۴/۱۵	شکرالله سالاریان	ایده‌آلهای اول مجانبی وابسته به فانکتورهای مشتق‌شده
پنجشنبه ۷۴/۴/۲۲	مسعود طوسی	همبافتهای کوزین و مدولهای کسره‌های تعمیم‌یافته
پنجشنبه ۷۴/۴/۲۹	خدیجه احمدی‌آملی	محاسبه مدولهای کوهمولوژی موضعی
دوشنبه ۷۴/۵/۲	سعید اکبری	جابه‌جاگرهای جمعی در حلقه‌های تقسیم
پنجشنبه ۷۴/۵/۱۲	سیامک یاسمی	ابعاد همولوژیک مدولها و یکرختی‌های طبیعی

مجل سخنرانیها: ساختمان اختیاریه

سخنرانی کاظم خشیارمنش در ساعت ۱۷ و بقیه سخنرانیها در ساعت ۱۶ برگزار خواهد شد.



United Nations  
Educational  
Scientific and Cultural  
Organization

  
Institute for Studies in  
Theoretical Physics  
and  
Mathematics

VIIth REGIONAL CONFERENCE ON  
MATHEMATICAL PHYSICS

## CASPIAN CONFERENCE

Oct. 15-22, 1995  
Bandar Anzali, Iran.

The Institute for Studies in Theoretical Physics and Mathematics (IPM) will organize the Seventh Regional Conference on Mathematical Physics (**Caspian Conference**) with the co-sponsorship of the United Nation Educational, Scientific and Cultural Organization.

Topics to be covered:

-String Theory	-Cosmology
-CFT	-Complex Systems
-Integrable Models	-Quantum Groups
-Phenomenology of Particle Physics	

Partial list of lecturers from outside of the region:

Louis Alvarez-Gaume (CERN)	Sanjay Jain (IISC, India)
Alexander A. Belavin (Landau Inst.)	Bahram Mashhoon (Missouri)
Robert Brandenberger (Brown)	Alexander Morozov (ITEP, Moscow)
Edward Corrigan (Durham)	Werner Nahm (Bonn)
Sumit R. Das (Tata)	Hossein Partovi (Sacramento)
John Ellis (CERN)	Seifollah Randjbar-Daemi (ICTP)
Cezar Gomez (Madrid)	Spenta Wadia (Tata)

Sponsored by  
UNESCO, International Center for Theoretical Physics,  
Ministry of Culture and Higher Education,  
Sharif University of Technology

Organizing Committee: F. Ardalan, H. Arfaei, S. Rouhani

Send all correspondence to:

Caspian Conference, IPM, P.O. Box 19395-5746, Tehran, Iran

E-mail: regconf@physics.ipm.ac.ir

Fax: +(9821)2280415, Tel: +(9821) 2280692 & 2290934

Hotel Sefid Kenar: Km 6, Anzali-Astara Road, Tel: +(98181)23032-5, Fax: +(98181)28023



## آنچه گذشت

از جمله مسائل مطرح شده موضوع زبان کنفرانس بود که نظر اکثریت بر آن شد که در سالهای آینده زبان کنفرانس فارسی باشد. البته این امر محدودیتهایی در مورد استفاده از سخنرانان و مدعوین خارجی به وجود خواهد آورد.

همچنین نظر جمع بر محدود کردن سخنرانها به یک ساعت بود که باز می تواند باعث شود برای بعضی مطالب فرصت توضیح کافی نباشد؛ قرار شد کمیته اجرایی کنفرانس نسبت به تغییرات زمان در موارد خاصی انعطاف نشان دهد.

شد. بحث و مذاکره در فواصل میان سخنرانها ادامه داشت.

همچون سال گذشته هر سخنرانی بر مبنای فعالیتهای پژوهشی سخنران بود، ولی کنفرانس با تعدادی میباحث غیر از فیزیک انرژیهای بالا، از جمله سخنرانیهایی در فیزیک پلاسما و ریاضیات محض، متنوعتر می نمود. در پایان روز دوم طی یک برنامه میزگرد در حضور شرکت کنندگان نحوه اجرای کنفرانس مورد ارزیابی قرار گرفت و رهنمودهایی برای اجرای کنفرانس در سالهای آینده ارائه شد.

## دومین کنفرانس بهاره فیزیک انرژیهای بالا

دومین کنفرانس بهاره فیزیک انرژیهای بالا در فاصله ۲۴ الی ۲۶ خرداد ماه امسال در بخش فیزیک در فرمانیه با شرکت حدود ۸۰ فیزیکدان و دانشجوی فیزیک برگزار شد.

در این کنفرانس نیز مانند سال گذشته تکیه بر مبادله نزدیک افکار و پرسش و پاسخ در جلسات سخنرانی بود. تعداد ۲۲ سخنرانی از ۹ صبح الی ۱۰ شب هر یک به مدت قریب به یک ساعت ایراد



فرهاد اردلان (مراسم افتتاحیه کنفرانس)

حالات گسسته سیاهچاله در نظریه ریسمان، فرهاد اردلان، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف. هم جوشی هسته ای و پیشرفت های اخیر، محمدرضا اسکندری، دانشگاه شیراز. توابع بری هولومورفیک، یوسف بهرام پور، دانشگاه کرمان.

تحصیلات تکمیلی در علوم پایه زنجان. ارتباط دگرگونی جردنی (۲)  $SL$  و دگرگونی  $q$  آن، امیر آقامحمدی، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه الزهرا. نظریه تابعی چگالی و ناهنجاری محوردار الکترودینامیک کوانتومی، فرشاد ابراهیمی، دانشگاه شهید بهشتی.

## سخنرانیهای دومین کنفرانس بهاره فیزیک انرژیهای بالا

بررسی قانون جمع گانفرید، فیروز آرش، دانشگاه صنعتی امیرکبیر. بررسی  $QCD$  روی شبکه به روش بسط بر حسب ضریب جفت شدگی قوی در دما و چگالی باریونی محدود، سیاوش آزاگف، مرکز

اثر کوانتومی هال روی سطوح غیر تخت، مسعود علیمحمدی، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه تهران.

تئوری‌های میدان توپولوژیک گسسته روی سطوح دوبعدی، وحید کریمی پور، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف.

ماده هسته‌ای در دمای معین، مجید مدرس، دانشگاه صنعتی امیرکبیر.

فاز بری، طبقه‌بندی کلاف، و نمایش گروه، علی مصطفی زاده، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف.

مدلی برای عالم با بعد دینامیکی، رضا منصور، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف.

نمایش بوزون آزاد جبر  $OSP(2/1)$  و  $Uq(OSP)(2/1)$ ، عزیزاللمه شفیع‌خانی، مرکز تحقیقات فیزیک نظری و ریاضیات.

سیستم‌های همبستگی کوانتومی، احمد شفیع‌ده‌آباد، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه تهران.

جرم یاریون‌های  $1/2$  و  $3/2$  در مدل سکرمی  $SU(4) \times SU(4)$ ، سیدموسی شیخ‌الاسلامی، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه تهران.

جفت شدن امواج در پلاسماهای طبقه‌بندی شده، بیژن شیخ‌الاسلامی سبزواری، مرکز تحقیقات فیزیک نظری و ریاضیات.

تقارنهای تعمیم‌یافته، محمدهادی صالحی کرمانی، مرکز تحقیقات فیزیک نظری و ریاضیات.

کوانتس بار الکتریکی و نمایشهای کمینه وایل به کمک حذف ناهنجاریها، منصوره پشنگ‌پور، دانشگاه صنعتی اصفهان.

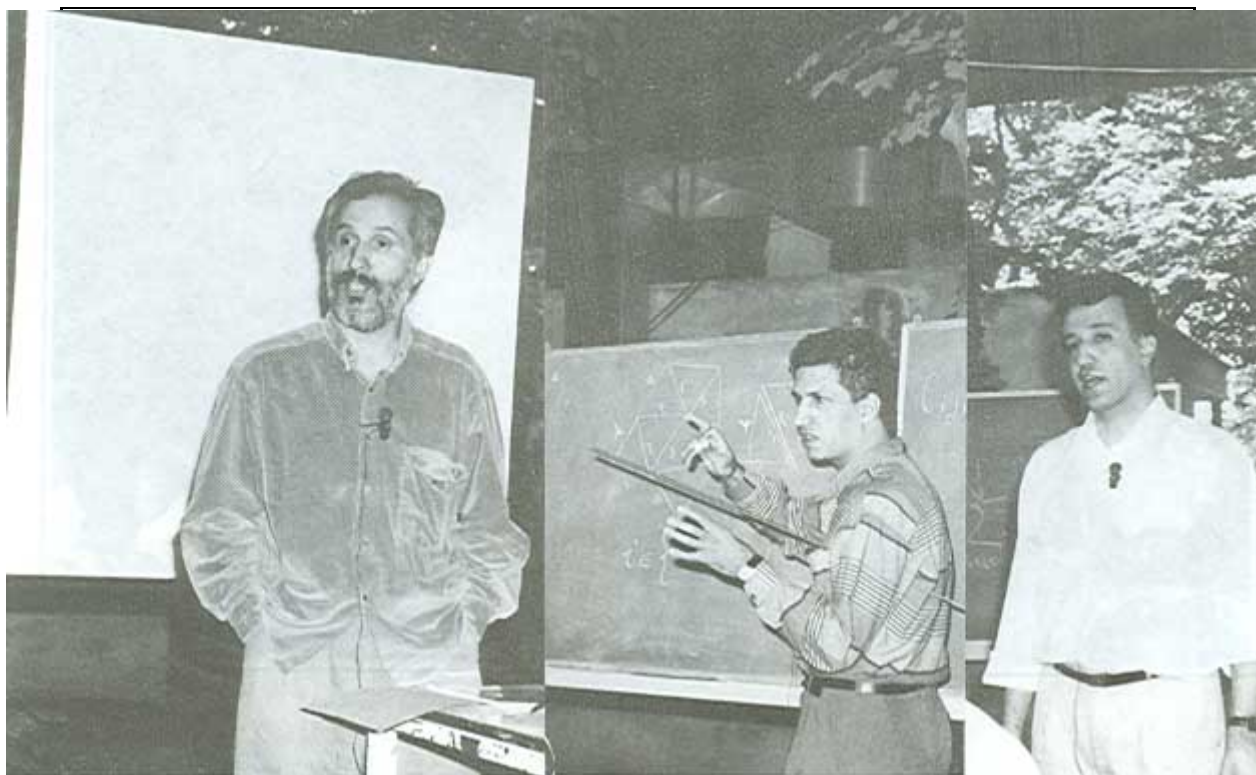
تابش زمینه در پلاسما، نودر تسمینتسواتزه، انستیتوی فیزیک گرجستان.

فاز مغناطیسی در مدل دریدا، شاهین روحانی، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف.

ماده تاریک سرد و سن خوشه‌های کروی، نعمت‌الله ریاضی، دانشگاه شیراز.

مدل تعمیم‌یافته شوئینگر در  $1+1$  بعد، مهدی سعادت، دانشگاه صنعتی اصفهان.

گروه کوانتومی پوانکاره دوبعدی، احمد شریعتی، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه تهران.



از راست به چپ: شاهین روحانی، وحید کریمی پور، رضا منصور

و دانشگاه تربیت مدرس، نظریه صدق کریپکی، احمد رضا شهیدی، دانشگاه علم و صنعت ایران، منطق فازی و کاربردهای آن، امیر دانشگر، دانشگاه صنعتی شریف.

شبکه بستار اندیسی مجموعه‌های کارآمد، فرزاد دیده‌ور، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف. توسعه‌های پایانی مدل‌های استقرای باز، مجتبی منیری، مرکز تحقیقات فیزیک نظری و ریاضیات

## سمینار هفتگی هسته منطق (شروع: بهار ۱۳۷۴)

نظریه‌های اهرن فوخت، مسعود پورمهدیان، مرکز تحقیقات فیزیک نظری و ریاضیات.

گروه اتومورفیزم‌های مجموعه‌های کارآمد، صالح عملی‌یاری، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف. نظریه مجموعه‌های غیرخوش‌بنیاد، روزبه شهرستانی، مرکز تحقیقات فیزیک نظری و ریاضیات. نظریه‌های کامل در مجموعه‌های پذیرفتنی، مسعود پورمه‌دیان، مرکز تحقیقات فیزیک نظری و ریاضیات.

### سمینار هفتگی هسته تحقیقاتی ترکیبیات و محاسبه (شروع: بهار ۱۳۷۴)

اسکیم‌های انجمنی (۱)، رضا ناصرعصر، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف. اسکیم‌های انجمنی (۲)، رضا ناصرعصر، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه صنعتی شریف. تولید درختان باینری، عباس نودزی، مرکز تحقیقات فیزیک نظری و ریاضیات و دانشگاه تهران. گروه‌های کاکسیترا، محمد جلوداری مسقانی، دانشگاه صنعتی شریف. الگوریتم جدیدی برای یافتن درخت فراگیر مینیموم، هایده اهرابیان، دانشگاه تهران.

### مسعود مرتضوی

مسعود مرتضوی، دارای درجه دکترا در شیمی و دانشجوی دکترا در منطق ریاضی در دانشگاه برکلی است. وی در بهار امسال طی سفری به ایران، به دعوت گروه منطق مرکز تحقیقات فیزیک نظری و ریاضیات یک سخنرانی با عنوان لزوم دوپستگی زمان در جملات شخصیه ایراد نمود.

### پروفسور تسینتساتزه در مرکز



پروفسور نودر تسینتساتزه از ۲۵/۱/۷۴ تا ۲۵/۴/۷۴ میهمان مرکز تحقیقات فیزیک نظری و ریاضیات بود. ذیلاً نوشته ایشان در معرفی خود می‌آید.

### زندگینامه

ملیت من گرجستانی است و کشور من جمهوری گرجستان است. ازدواج کرده‌ام و صاحب دو فرزند هستم. فوق لیسانس خود را در فیزیک از دانشگاه ایالتی تفلیس گرفتم (ژوئن ۱۹۵۵). دوره دکترا را در سالهای ۱۹۵۸-۱۹۵۵ در دانشگاه ایالتی خارکف با نظارت پروفسور آخیزر گذراندم و دکترای خود در سال ۱۹۵۸ گرفتم. در سال ۱۹۶۵ نیز به سمت استادی در دانشگاه ایالتی تفلیس ارتقاء یافتم.

هم‌اکنون سرپرست گروه فیزیک پلاسما در انستیتوی فیزیک آکادمی علوم گرجستان، سرپرست گروه فیزیک پلاسما در دانشگاه ایالتی تفلیس، عضو مجمع مسائل فیزیک پلاسما روسیه، و رئیس مجمع پلاسما گرجستان و مجمع هماهنگی تحقیقات لیزر در علوم و تکنولوژی گرجستان هستم. همچنین عضو هیأت برنامه‌ریزی و کمیته برنامه‌های بین‌المللی سمپوزیمها و کنفرانسها و کارگاهها در چندین کشور و سرپرست همکار کالج بهاره فیزیک پلاسما (تریست، ایتالیا) در ۱۹۸۹، ۱۹۹۱، ۱۹۹۳ بوده‌ام.

### زمینه‌های فعالیت

بخش فیزیک پلاسما انستیتوی فیزیک در این زمینه‌ها تحقیقات نظری و تجربی انجام می‌دهد:

۱. ساختارهای شارلولة غیرخطی و تأثیرات آن بر فرآیند انتقال الکترون در میدانهای متقاطع الکتريکی و مغناطیسی در پلاسما الکترونی با مغناطیس جبران‌نشده.

۲. هولوگرافی IF برای  $\lambda = 106 \text{ mkm}$

- تداخل‌سنجی هولوگرافی IF برای تشخیص وضعیت پلاسما.

- مواد مربوط به ضبط اطلاعات در حیطه  $\lambda = 106 \text{ mkm}$ .

- تصویرهای سه بعدی اجسامی که در ناحیه مرئی غیرشفاف‌اند.

۳. پلاسما و پدیده‌های هیدرودینامیک مربوط به شکست اپتیکی در گازها و مکانیسمهای انتشار جبهه‌های یونیده، خودکانونی کردن.

۴. ساخت چشمه‌های مولد کپه‌هایی از پلاسما قوی‌یونیده بدون برخورد در خلاء، و پلاسما فتیونیده در دمای کم و فشار زیاد. از این وسایل می‌توان برای حل مسائل مربوط به CTR، لیزرهای گازی پر قدرت، شیمی پلاسما، و عملیات مواد استفاده کرد.

۵. شبیه‌سازی فرآیندهای دینامیکی گازها در سیستمهایی که برای گرم کردن پلاسما به‌کار می‌روند. از جمله این فرآیندها فشردگی مغناطیسی پلاسما، کانونی کردن پلاسما، و اثر پرتو لیزر حلقوی بسیار قوی بر مواد است. مطالعه حرکت جمعی امواج ضربه‌ای بدون بعد که دارای تقارن استوانه‌ای‌اند.

۶. تحقیقات تجربی تأثیرات غیرخطی امواج الکترومغناطیسی روی پلاسما فعال مغناطیسی، توسعه روشهای HF و UHF برای گرم کردن پلاسما.

## المپیادها در مرکز

طبق رسم هر ساله دانش‌آموزان منتخب شرکت‌کننده در المپیادهای مختلف در روز ۲۹ خرداد میهمان مرکز بودند. پس از صرف نهار و بازدید از کتابخانه و آشنایی مختصر با پست الکترونیک، دکتر محمدجواد لاریجانی رئیس مرکز به جمع حاضران پیوست. خلاصه‌ای از سخنان ایشان در زیر آمده است.

به دوستان خوش‌آمد می‌گویم. در واقع این مرکز برای سرمایه‌گذاری روی استعدادهای قابلی که دلشان می‌خواهد وقتشان را صرف ریاضیات و فیزیک بکنند تأسیس شده است. اینک در کشور ما دانشگاه‌های زیادی در مناطق مختلف وجود دارد؛ دانشگاه آزاد هم فارغ‌التحصیلان زیادی داشته است، که از نظر اجتماعی چیز بدی نیست، و آثار خوب اجتماعی هم دارد. اما این کار برای توسعه علمی کافی نیست، یعنی بیشتر از جنبه اجتماعی و شکل دادن به ساختار اجتماعی کشور است. برای توسعه علمی حتماً ما مجبوریم که روی

آنهایی که خیلی نخبه باشند سرمایه‌گذاری کنیم. در واقع مرکز تحقیقات با یک چنین اندیشه‌ای به‌وجود آمده تا بیشتر روی این افراد سرمایه‌گذاری شود. پس آن هدف عمده‌ای که ما در اینجا دنبال می‌کنیم تولید انبوه نیست، یعنی برای ما افراد هر کدام شخصاً مطرح هستند. ما دانشجویان را نمی‌بینیم، تک‌تک افراد را می‌بینیم - در مورد علما و دانشمندانمان هم همین‌طور. به عکس سیستم آموزش عمومی کشورمان، برای هر فرد پرونده خاصی درست کرده‌ایم و او را به‌صورت فردی مورد حمایت قرار می‌دهیم.

به هر صورت امیدواریم در میان شما در آینده کسانی پیدا شوند که پرچم علم را از آن چیزی که هست خیلی بالاتر ببرند، ان شاء الله. شاید آن مقاله مرا خوانده باشید که در آستانه برنامه دوم راجع به ثروت ملی نوشته بودم: از وقتی که نفت درآمد، ثروت ملی برای ما چاههای نفت شد: هر جا که چاه نفت بود چندین میلیون دلار پول ریختیم و استخراج کردیم و فکر کردیم این، ثروت به‌همراه

می‌آورد - البته همین امر هم باعث بدبخت بودنمان بوده و باعث عقب‌ماندگی - در حالی که ثروت ملی استعدادها خوب کشور هستند - آنهایی هم که در تجارت و تولید پیشرفت می‌کنند جزو استعدادها خوب هستند. استعدادها خوب را هم باید مثل چاههای نفت استخراج کرد و به آنها رسید و امکانات داد، و این تصویری است که من فکر می‌کنم که در کشور به آن دامن زده می‌شود و ان شاء الله روی آن سرمایه‌گذاری می‌شود.

به هر صورت ما آرزویمان این است که ده سال دیگر وقتی کتابهای درسی ریاضیات را ورق می‌زنیم، در کنار قضایای مختلفی که با اسمی مختلف است اسمهای شما هم نوشته شده باشد. می‌خواهیم شما حوزه‌های علمی تشکیل بدهید و زیر نظر شما دهها دانشجو رشد پیدا کنند، و خلاصه، پرواز کردن را هم یاد بگیرید و هم به دیگران یاد بدهید. این آرزوی ماست و تا جایی که قدرت داریم برای آن تلاش می‌کنیم. شما را از ته دل دعا می‌کنیم که موفق بشوید.



از راست به چپ، ایستاده: یحیی تابش، عزیزالله رخشان، محمد جواهری، رضا صادقی، حسن زوری، غلامرضا بردارن‌خسروشاهی، سیاوش شهشهبانی، ماشالله ترحمی، روزه کیانی، محمدرضا صلواتی‌پور، علی جلالی، محمد مهدیان، مهران مهر.

از راست به چپ، نشسته: مریم میرزاخانی، رویا بهشتی‌زواره، محمدعلی آقام، رضا شاه‌اکبری، بابک فرزاد، روزه یونادار، کیوان ملاحی.



## انتشارات مرکز

### گزارشهای فنی

**A. Nowzari-Dalini**

IPM-95-084

*The lower and upper bounds for generalized section functors*

**S. Yassemi**

IPM-95-085

*Does Bell's inequality violation imply non-locality?*

**H. Razmi and**

**M. Golshani**

IPM-95-086

*Quantum group symmetry of the quantum Hall effect on the non-flat surfaces*

**M. Alimohammadi and**

**A. Shafei Deh Abad**

IPM-95-087

*2-d Gravity as a limit of the  $SL(2, R)$  black hole*

**M. Alimohammadi and**

**F. Ardalan**

IPM-95-088

*Application of a neural network to the prediction of transmembrane regions of membrane proteins*

**C. Lucas, A. Tabesh,**

**and S. Khademi**

IPM-95-089

*A new svd-based doa estimation method*

**D. Dabiri and C. Lucas**

**C.E. Praeger**

IPM-95-076

*Quantified modal logic: an analysis of certain essentialist theses*

**H. Vahid**

IPM-95-077

*Endomorphisms of the group of all recursive permutations*

**A.S. Morozov**

IPM-95-078

*Free field representation of  $osp(2|1)$  and  $U_q(osp(2|1))$*

**W.S. Chung and**

**A. Shafiekhani**

IPM-95-079

*Generalized Camacho-Sad theorem*

**B. Khanedani**

IPM-95-080

*On the group  $G(D) = D^*/RN_{D/F}(D^*).D'$*

**S. Akbari**

IPM-95-081

*Hypersurfaces in  $\mathbb{R}_1^N$  satisfying  $\Delta x = Ax + B$*

**S.M.B. Kashani**

IPM-95-082

*A critique of two construction methods of  $t$ -designs*

**G.B. Khosrovshahi**

IPM-95-083

*Generation of binary trees from new (0-1) codes*

**H. Ahrabian and**

IPM 94-069

*First variation of holomorphic forms and some applications*

**B. Khanedani**

IPM 94-070

*Octahedrals in Steiner quadruple systems*

**G.B. Khosrovshahi and**

**H. Yousefi-Azari**

IPM 94-071

*On a conjecture of A. Hartman*

**S. Ajoodani-Namini and**

**G.B. Khosrovshahi**

IPM 94-072

*On (2, 3)-trades of small volume*

**G.B. Khosrovshahi and**

**H. Maimani**

IPM 94-073

*A general formulation of discrete-time quantum mechanics restrictions on the action and the relation of unitarity to the existence theorem for initial-value problems*

**M. Khorrami**

IPM 94-074

*A triangular deformation of the two dimensional Poincaré algebra*

**M. Khorrami, A. Shariati,**

**M.R. Abolhassani, and**

**A. Aghamohammadi**

IPM 94-075

*Movement and separation of subsets of points under group actions*

نسخه‌هایی از انتشارات مرکز تحقیقات فیزیک نظری و ریاضیات موجود است؛ علاقه‌مندان می‌توانند برای دریافت آنها با نشانی زیر مکاتبه کنند:  
تهران -  
صندوق پستی ۱۷۹۵-۱۹۳۹۵، واحد انتشارات مرکز تحقیقات فیزیک نظری و ریاضیات.

## گزارشی از کتابخانه مرکز

در پایان خرداد ماه موجودی کتابخانه به شرح زیر بوده است:

• ۱۱۶۶۵ عنوان کتاب

• ۴۱۲ عنوان نشریه ادواری مرکب از:

– ۱۰۰ عنوان نشریه ادواری با تمام شماره‌های پیشین.

– ۸۰ عنوان نشریه ادواری با شماره‌های پیشین از سال ۱۹۸۹ و ۱۹۸۸.

– ۲۳۲ عنوان نشریه ادواری با شماره‌های پیشین از سال ۱۹۹۰ به بعد.

در ضمن پیشینه ۲۲ عنوان از نشریات به صورت میکروفیلم موجود است.

در پایان بهار ۱۳۷۴ تعداد اعضای کتابخانه به ۷۵۰ نفر بالغ گردیده است. ساعات کار کتابخانه:

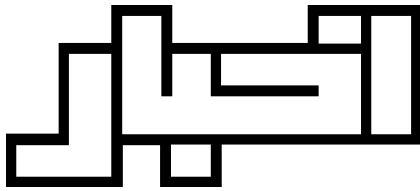
شنبه تا چهارشنبه از ۸ تا ۱۸،

پنجشنبه از ۸:۳۰ تا ۱۵:۴۵.

## برنامه‌های فصل

### برنامه سمینارهای ادواری

- سمینار فیزیک، چهارشنبه‌ها ساعت ۱۶، ساختمان فرمانیه.
- سمینار هسته فیزیک بنیادی، دوشنبه‌ها ساعت ۱۰، ساختمان فرمانیه.



اخبار، نشریه خبری مرکز تحقیقات فیزیک نظری و ریاضیات، در آغاز هر فصل منتشر می‌شود. آراء مندرج در اخبار لزوماً مبین نظر رسمی مرکز نیست. نقل مطالب بدون ذکر مأخذ ممنوع است.

صاحب امتیاز مرکز تحقیقات فیزیک نظری و ریاضیات

مدیر مسئول غلامرضا برداران خسروشاهی

ویراستار بنیامین کاویانی

مدیر داخلی عالیبه ارفعی

مسئول تهیه خبر آناهیتا سمیع

حروفچینی  $\text{\TeX}$ -پاک

مانیلا حاج سلیمی

ناظر چاپ نادر کشری

همکار فنی شرکت انتشارات علمی و فرهنگی

واحد انتشارات نشانی

مرکز تحقیقات فیزیک نظری و ریاضیات

تهران - اختیاریه شمالی، بن بست مهران،

صندوق پستی ۱۷۹۵-۱۹۳۹۵

تلفن ۲۵۴۳۸۶۰-۲۲۸۷۰۱۳

پست الکترونیکی ipmpub@rose.ipm.ac.ir

### سمینارهای بخش ریاضی

تابستان ۱۳۷۴

۷۴/۴/۲۰	فریدون شهیدی، قضیه آخر فرما
۷۴/۴/۲۶	امین شکراللهی، محاسبه شاخصهای نامنظمی در اعداد اول
۷۴/۵/۲	مجتبی منیری، استقلال/سازگاری چند قضیه/حدس مشهور از/با یک نظریه ضعیف اعداد
۷۴/۵/۹	فرانسوا مورا، آشنایی با نظریه همگون سازی [به انگلیسی]
۷۴/۵/۱۶	محمد اردشیر بهرستاقی، نشان دادن منطق شهودگرایی در منطق پایه
۷۴/۵/۲۳	هنریک شاهقلیان، تعمیمی از نظریه منظم بودن کافارلی

زمان : ساعت ۱۶:۰۰

مکان : ساختمان اختیاریه