در پایان دوست دارم که با یک خاطره از یک گفتمان مدیر موفق مطلب خود را تمام کنم. در یک سخنرانی که به دعوت گروه ریاضی کاربری جهت ایجاد انگیزه برای دانشجویان ریاضی مهیا شده بود شرکت کرده بودم. سخنران یک مدیر موفق با تحصیلات کارشناسی ریاضی و ارشد مدیریت بودند. مطلب بسیار جالب سخنرانی این بود که سخنران تمام موفقیتش را مدیون تفکر ریاضی می‌دانسته که در طول چهار سال تحصیل در رشته ریاضی از دنیای ریاضیات دریافت کرده بود. و این نتیجه حضور یک ذهن ریاضی در عرصه‌های علمی دیگر است.

فریبا بهرامی
دانشگاه تبریز

★ ★ ★

فراخوان جایزه دکتر هشترودی

به اطلاع همکاران ارجمند می‌رسانم علاوه بر مقالات ارائه شده در سمینار هندسه و توپولوژی که در دانشگاه بناب برگزار شده، مقالاتی که در زمینه هندسه و توپولوژی در مجلات معتبر و در سال‌های ۲۰۱۰ و ۲۰۱۱ به چاپ رسیده‌اند نیز می‌توانند نامزد دریافت جایزه هشترودی باشند. همه علاقه‌مندان در این زمینه در صورت تمایل می‌توانند pdf مقالات خود را تا پایان اسفندماه سال ۱۳۹۰ به نشانی azarpanah@ipm.ir ارسال کنند. در ضمن مقالات برتر ارائه شده در سمینار فوق توسط کمیته علمی سمینار بررسی و به هیأت امنای جایزه دکتر هشترودی تحویل داده شده است و نیازی به ارسال آن‌ها نیست.

فریبرز آذرپناه
رئیس هیات امنای جایزه دکتر هشترودی

کاربردهایی از گروه‌های ساده متناهی

شریل ای. پرگر

چکیده

انشعاباتی از رده‌بندی گروه‌های ساده متناهی، که یکی از بزرگ‌ترین پیروزی‌های قرن بیستم در ریاضیات است، هنوز هم باعث پیشرفت‌های پیشگامانه بسیاری در زمینه‌های ریاضیات می‌شود. در این یادداشت چندین کاربرد کلیدی این رده‌بندی مورد بحث قرار می‌گیرد.

رده‌بندی گروه‌های ساده متناهی که در فوریه سال ۱۹۸۱ میلادی توسط دانیل گورنستاین اعلام شد یکی از بزرگ‌ترین پیروزی‌ها در ریاضیات، در اواخر قرن بیستم بود، و تا امروز انشعابات آن در بسیاری از زمینه‌های ریاضیات دیده می‌شود. فهرست گروه‌های سادهٔ متناهی با کمال تعجب کوتاه است: گروه دوری مرتبه اول p که با C_p نمایش داده می‌شود، گروه متناوب $\mathbb{A}_n$، $n \geq 5$ که گروه همه جایگشت‌های زوج یک مجموعه n عضوی می‌باشد، تعداد متناهی از خانواده نامتناهی گروه‌های ساده که گروه‌های ساده نوع لی نامیده می‌شوند، و دقیقاً ۲۶ گروه سادهٔ دیگر که به گروه‌های پراکنده معروفند و بزرگترین آن‌ها هیولا نامیده می‌شود که گروهی است از مرتبهٔ

$$808017424794512875886459904961710757005754324360000000000.$$

قبل از اعلام نتیجه رده‌بندی در سال ۱۹۸۱ میلادی، نتایجی از آن منتظر فرصت ظهور بودند. به‌عنوان مثال، می‌توانستیم فهرستی از گروه‌های جایگشتی که تحت آن‌ها هر زوج از نقاط هم‌ارزند را ارائه دهیم (گروه‌های جایگشتی ۲ ـ انتقالی) [۳].

۱. گروه‌های ساده و نظریه جبری گراف

پس از گذشت سال‌ها معلوم نبود که رده‌بندی گروه‌های ساده بتواند به‌طور موفقیت‌آمیزی باعث حل مسائل دیگر شود. یکی از مشهورترین این مسائل، حدسیه‌ای بود از چارلز سیمز که در سال ۱۹۶۵ میلادی مطرح گردید و ارتباطی بین نظریه گروه‌های جایگشتی و نظریه گراف برقرار می‌کرد. و این سؤالی دربارهٔ گروه‌های جایگشتی اولیه بود. به همان نحوی که گروه‌های ساده متناهی آجرهای ساختمانی برای گروه‌ها هستند (عوامل ترکیبی)، گروه‌های اولیه نیز آجرهای ساختمانی گروه‌های جایگشتی را تشکیل می‌دهند. سیمز حدس زد که تابع f با دامنه اعداد

طبیعی وجود دارد به‌طوری‌که برای یک گروه جایگشتی اولیه که در آن پایدارساز یک نقطه H دارای مداری به طول d است، عدد کاردینال H حداکثر $f(d)$ می‌باشد. به زبان نظریه گراف حدسیه فوق چنین است: برای یک گراف رأس ـ اولیه یا گراف جهت‌دار از درجهٔ d (یعنی هر رأس به d رأس دیگر متصل است)، حداکثر $f(d)$ خودریختی (جایگشت‌های یال ـ پایا) وجود دارد به‌طوری‌که هر رأس داده شده را ثابت نگه می‌دارند. اثبات حدسیهٔ سیمز که در سال ۱۹۸۳ میلادی در [۵] ظاهر شد به اطلاعاتی دربارهٔ ساختار زیرگروهی گروه‌های سادهٔ نوع لی، و یکی از کاربردهای نابدیهی رده‌بندی گروه‌های ساده نامتناهی در نظریه جبری گراف نیاز داشت، (٦، بخش ۴۰۸c) را ببینید. رهیافت جدید در [۵] بعداً به یک چهارچوب استاندارد برای کاربرد رده‌بندی گروه‌های ساده متناهی در بسیاری از مسائل دربارهٔ گروه‌های جایگشتی اولیه و گراف‌های رأس ـ اولیه تبدیل گردید.

کاربردهای عالی و جدید رده‌بندی گروه‌های ساده در نظریه جبری گراف هنوز هم ادامه دارد، و بسیاری از کاربردهای جدید با نتایج عمیقی دربارهٔ ساختار و خواص گروه‌های ساده همراه هستند. جدیدترین این کاربردها مربوط به گراف‌های منبسط (expander) است و این‌ها عبارتند از گراف‌ها یا شبکه‌هایی که هم‌زمان تُنُک و خیلی همبند می‌باشند. این گراف‌ها کاربردهای مهمی در طرح‌ها و تجزیه و تحلیل شبکه‌های نیرومند ارتباطات دارند. در [۱۱] مروری از این کاربردها در نظریهٔ تصحیح خطای کدها، نظریه شبه تصادفی، و بسیاری دیگر از این کاربردها به طرز زیبایی آورده شده است. یک خانواده از گراف‌های متناهی، که همگی از درجهٔ یکسانی هستند ولی شامل گراف‌ها از هر اندازهٔ دلخواه می‌باشند، یک خانوادهٔ منبسط (expander) نامیده می‌شود اگر ثابت c وجود داشته باشد به‌طوری‌که نسبت $\frac{|\partial A|}{|A|}$ به ازای هر زیرمجموعهٔ A از مجموعهٔ رئوس گراف Γ در خانواده، حداقل مساوی c باشد، جایی که A شامل حداکثر نیمی از رئوس Γ بوده و ∂A مجموعه رئوس Γ به فاصلهٔ ۱ از A می‌باشد. از جدیدترین نتایج چنین استنباط می‌گردد که خانوادهٔ زیادی از گراف‌های کیلی روی گروه‌های ساده نوع لی با رتبه کراندار، جزو خانواده‌های منبسط (expander) می‌باشند. این فعالیت‌های ناگهانی با نتایج قاطع و عالی هلفگات[۹] در سال ۲۰۰۸ میلادی دربارهٔ گروه خطی تصویری $\mathrm{PSL}(۲,p)$ که p عدد اول است، آغاز گردید. قوی‌ترین نتایج جدید دربارهٔ گروه‌های نوع لی با رتبه کراندار عبارتند از نتایج جدیدی دربارهٔ «رشد در گروه‌ها» توسط پیبروزابو [۱۹]، و مستقلاً توسط بروئیلارد، گرین و تائو در [۲] برای گروه‌های شواله متناهی.

۲. گروه‌های ساده، اعداد اول و جایگشت‌ها

تعدادی از نتایج، دربارهٔ گروه‌های جایگشتی دارای بیانی «ساده» هستند که در آن‌ها ذکری از گروه‌های ساده نمی‌شود، اما اثبات شناخته شدهٔ آن‌ها به رده‌بندی گروه‌های ساده بستگی دارد، که البته این نظریهٔ گروه‌های ساده‌ای است که مدت‌های مدیدی پس از اعلام رده‌بندی، مورد مطالعه قرار گرفت. در واقع بسیاری از نتایج اخیر در این زمینه نیازمند فهم عمیق و دقیق گروه‌های ساده متناهی، به‌ویژه ساختار زیرگروهی، آمار عناصر، و نمایش‌های آن‌ها می‌باشد.

یک ارتباط تعجب‌برانگیز بین تعداد اعداد اول و گروه‌های ساده متناهی به فاصله اندکی پس از اعلام رده‌بندی کشف گردید. این نتیجه متعلق به کمرون، نیوتن و تیگو است که در سال ۱۹۸۲ میلادی در مرجع [۴] چاپ شد. هر عدد صحیح و مثبت $n \geq ۵$ به‌عنوان اندیس یک زیرگروه ماکسیمال از یک گروه ساده ظاهر می‌گرد، یعنی در واقع گروه سادهٔ متناوب $\mathbb{A}_n$ دارای زیرگروه ماکسیمال $\mathbb{A}_{n-۱}$ از اندیس $n = \frac{|\mathbb{A}_n|}{|\mathbb{A}_{n-۱}|}$ است.

گوییم n یک اندیس ماکسیمال است هرگاه $n = \frac{|G|}{|H|}$، جایی‌که G یک گروه سادهٔ ناآبلی و H یک زیرگروه ماکسیمال G که $(G,H) \neq (\mathbb{A}_n, \mathbb{A}_{n-۱})$ می‌باشند. در مرجع [۴] ثابت شده که اگر $x \to \infty$ آنگاه

$$\frac{\max(\mathrm{x})}{\pi(\mathrm{x})} \to ۱,$$

جایی‌که $\max(x)$ تعداد اندیس‌های ماکسیمال حداکثر x و $\pi(x)$ تعداد اعداد اول حداکثر x می‌باشد. چگال حدی مجموعهٔ اندیس‌های ماکسیمال با توجه به این واقعیت شرح داده می‌شود که، به ازای هر عدد اول p، گروه تصویری خاص $\mathrm{PSL}(۲,p)$ روی خط تصویری $PG(۱,p)$ از مرتبهٔ $p+۱$ اولیه عمل می‌کند، و لذا دارای زیرگروه ماکسیمال از اندیس $p+۱$ است. انگیزهٔ عمده‌ای که باعث یافتن این نتیجه گردید کاربرد آن در گروه‌های جایگشتی اولیه بود، هم‌چنین در مرجع [۴] ثابت گردید:

تعداد $D_{\mathrm{prim}}(x)$ اعداد صحیح n که برای آن‌ها یک گروه جایگشتی اولیه روی n حرف وجود دارد (یعنی یک گروه جایگشتی درجه n)، به جز S_n و $\mathbb{A}_n$، در تساوی زیر صدق می‌کند:

$$\lim_{x\to\infty} \frac{D_{\mathrm{prim}}(x)}{\pi(x)} = ۲.$$

به جز عمل اولیهٔ $\mathrm{PSL}(۲,p)$ از درجهٔ $p+۱$، گروه دوری C_p اولیه از درجهٔ p است، و لذا در چگالی حدی نسبت ۲ محاسبه

می‌شوند. دو دههٔ بعد به همراه هیث ـ برتون و شالو در مرجع [۸] این نتیجه را به مبحث گروه‌های جایگشتی اولیه تعمیم دادیم، که این‌ها عبارتند از یک خانواده گروه‌های جایگشتی اکیداً بزرگتر از گروه‌های جایگشتی اولیه که در کاربردهای ترکیبیاتی با اهمیت‌اند. (یک گروه جایگشتی شبه اولیه نامیده می‌شود، هرگاه هر زیرگروه نرمال نابدیهی‌اش انتقالی باشد. هر گروه جایگشتی اولیه دارای این خاصیت است و بسیاری از دیگر گروه‌های جایگشتی نیز دارای این خاصیت هستند).

کمیتی حیاتی که ما برای معین کردن رفتار در جهت یک گروه جایگشتی شبه اولیه نیاز داشتیم عبارت بود از تعداد $\mathrm{sim}(x)$ از اندیس‌های ساده حداکثر x، جایی که بنا به تعریف ساده عبارت است از اندیس $\frac{|G|}{|H|}$ از زیرگروه دلخواه H از یک گروه سادهٔ ناآبلی G با شرط $(G,H) \neq (\mathbb{A}_n, \mathbb{A}_{n-1})$. ما ثابت کردیم که وقتی که $x \to \infty$ نسبت $\frac{\mathrm{sim}(x)}{\pi(x)}$ نیز دارای حد است و ثابت کردیم این حد برابر است با:

$$h = \sum_{n=1}^{\infty} \frac{1}{2\phi(2n)} = 1.76308500\ldots,$$

جایی که $\phi(m)$ عبارت است از تابع ـ فی اویلر، یعنی تعداد اعداد صحیح و مثبت حداکثر m و نسبت به m اول. نتیجه مشابه (که انگیزه اصلی ما برای مطالعهٔ $\mathrm{sim}(x)$ بود) عبارت از این بود که نسبت $\frac{D_{\mathrm{qprim}}(x)}{\pi(x)}$ به سمت $1+h$ میل می‌کند، وقتی که $x \to \infty$، جایی که $D_{\mathrm{qprim}}(x)$ تعداد گروه‌های جایگشتی شبه اولیه درجهٔ $n \leq x$، به جز S_n و $\mathbb{A}_n$ است. در این حالت هم، این نسبت‌ها با استفاده از زیرگروه‌های مختلف گروه ساده $\mathrm{PSL}(2,p)$ محاسبه شده‌اند.

همواره مثال دوست‌داشتنی از یک نتیجهٔ عمیق با بیانی ساده و فریب‌آمیز برای من منسوب به نتیجه‌ای از آیزاکس، کانتور و اسپالتن استاین در مرجع [۱۲] بوده است که در سال ۱۹۹۵ میلادی چاپ گردید: فرض کنید G یک گروه جایگشتی روی مجموعه‌ای n عضوی و p مقسوم‌علیه اولی از مرتبهٔ G است؛ در این صورت شانس این‌که یک عضو به تصادف توزیع شدهٔ G دارای دوری به طول مضربی از p باشد حداقل 1 به n می‌باشد. فرضیات این نتیجه کاملاً کلی هستند و هیچ اشاره‌ای بر این‌که ارتباطی با گروه‌های ساده دارد در آن‌ها مشهود نیست. با این وجود، تنها برهان ارائه شدهٔ این نتیجه بستگی به رده‌بندی گروه‌های ساده متناهی دارد، و در آن به‌ویژه از اطلاعات دقیق درباره گروه‌های وایل و چنبره‌های ماکسیمال در گروه‌های ساده متناهی نوع لی استفاده می‌شود، من اخیراً با آلیس نیمیر و سایرین کار کرده‌ام و کوشش داشته‌ام بفهمم که شرایط دقیق لازم برای مؤثر بودن این رهیافت چیست؟ ما یک روش تقریبی در [۱۶] یافتیم و از آن برای پایه‌ریزی چندین الگوریتم مونت کارلو در محاسبه با گروه‌های ساده نوع لی استفاده نمودیم (در مراجع [۱۴] و [۱۵])، حاصل کار تقریب‌های دقیق‌تر برای انواع عناصر گروه‌های سادهٔ نوع لی نسبت به رهیافت هندسی گروه‌های متناوب بود.

۳. گروه‌های ساده و برگردان‌ها

یکی از اولین نشانه‌هایی که فهمیدن گروه‌های متناهی ممکن است مسأله‌ای قابل پیگیری باشد نتیجهٔ دوران ساز «مقالهٔ مرتبه فرد» منسوب به فایت و تامپسون [۷] در سال ۱۹۶۳ میلادی بود که آن‌ها ثابت کردند هر گروه متناهی از مرتبهٔ فرد حل‌پذیر است، یا به‌طور معادل، هر گروه ناآبلی ساده و متناهی دارای عنصر ناتهی x است به‌طوری‌که $x^2 = 1$. چنین عنصری یک برگردان نامیده می‌شود، و نتیجهٔ فایت تامپسون، که هر گروه ناآبلی ساده و متناهی شامل برگردان است، بیش از ۵۰ سال قبل از این توسط برنساید در سال ۱۹۱۱ به‌صورت حدس بیان شده بود. مرکز ساز یک برگردان مانند x شامل آن دسته عناصر g از گروه است که با x جابه‌جا می‌شوند، یعنی $gx = xg$. مرکزساز برگردان‌ها در گروه‌های سادهٔ متناهی زیرگروه‌هایی هستند که در آن‌ها غالباً گروه‌های ساده کوچکتری حضور دارند. چندین مرحلهٔ حساس در رده‌بندی گروه‌های ساده شامل تجزیه و تحلیل سازماندهی شدهٔ مرکزساز یک برگردان در گروه‌های ساده بود، که نتیجهٔ آن عبارت بود از یک سری طولانی از مقالات عمیق و دشوار که گروه‌های ساده شامل انواع مختلف مرکزساز برگردان را سرشت‌نمائی می‌کرد.

اطلاعات مهمی دربارهٔ گروه‌های ساده را می‌توان با محاسبه پیدا کرد، و کلید آن روش‌های مؤثر برای ساختن مرکزسازهای برگردان‌هاست. برای ساختن یک برگردان، ابتدا به‌طور تصادفی عضوی از مرتبهٔ زوج می‌یابیم که توانی از آن یک برگردان است، سپس از الگوریتم ساخته شده توسط بری در [۱] استفاده کرده و مرکزساز آن را می‌سازیم. این روش‌ها به حد عالی و در عمل در محاسبه با گروه‌ای ساده پراکنده کارائی داشت. تعمیم کلی‌تری از روش بری در الگوریتم ثابت شدهٔ مونت ـ کارلو در مورد گروه‌های ساده نوع لی روی میدان‌ها با مشخصهٔ فرد مستلزم تخمین‌های حساس از عناصر گوناگونی در گروه‌های ساده است ـ ابتدا در مقالهٔ اثرگذار [۱۷] که توسط پارکرو ویلسون نوشته شده است (که سال‌ها قبل از چاپ آن به‌صورت پیش‌چاپ در دسترس بود)، و سپس با جزئیات کامل در مرجع [۱۰] این تقریب‌ها و محاسبات پیچیده کران پائینی روی اجرای الگوریتم می‌گذارد، اما با واقعیت‌های اجرای

عملی مطابقت ندارد. برنامهٔ وسیعی در مرحلهٔ آموزش است که یک تحلیل واقعی پیدا شود و قسمت اول تکمیل شده است [۱۴ و ۱۸].

رده‌بندی گروهای ساده متناهی قطرهٔ آبی برای پژوهش در زمینه‌های جبر، ترکیبیات، و سایر شاخه‌های ریاضیات بود. اثبات آن تقریباً به‌طور کامل مسأله مورد مطالعه و روش‌های آن را دچار تحول نمود. برای تشخیص بیشتر توان رده‌بندی در کاربردهای آتی، اطلاعات کامل دربارهٔ گروه‌های ساده مورد نیاز است ـ و این به‌عنوان یک نظریه جدید و هم‌چنین پیشرفت‌های محاسباتی حاصل خواهد شد.

[1] N. Bray, An improved method for generating the centeralizer of an involution, *Arch Math.* (Basel) 74(2000) 241-245.

[2] E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups, *Geometric and functional Analysis* (to appear), arXiv:1005.1881v1.

[3] P. J. Cameron, Finite permulation groups and finite simple groups, Bull. London Math. Soc. 13 (1981). 1-22.

[4] P. J. Cameron, P. M. Neumann and D. N. Teague, On the degrees of primitive permutation groups, *Math. Zeit.* 180(1982) 141-149.

[5] P. J. Cameron, C. E. Praeger, G. M. Seitz and J. Saxl, On the Simś conjecture and distance transitive graphs, Bull. Lond. *Math. Soc.* 15 (1983) 499-506.

[6] D. Dixon and B. Mortimer, *Permulation Groups* (Springer, 1996).

[7] W. Feit and J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* 13 (1963) 775-1029.

[8] D. R. Heath-Brown, C. E. Praeger and A. Shalev, Premutation grups, simple groups and sieve methods, *Israel J. Math.* 148(2005) 347-375.

[9] H. A. Helfgott, Growth and generation in $SL_2(Z/pZ)$, *Annalsf Math,* 167 (2008) 601-623.

[10] P. E. Holmes, S. A. Linton, E. A.ÓBrien, A. J. E. Ryba and R. A. Wilson, Constructive membership in black-box groups, *J. Groups Theory* 11 (2008) 747-763.

[11] S. Hoory, N. Linial and A. Widgerson, Expander graphs and their applications, Bull. *Amer. Math. Soc.* 43 (2006) 439-561.

[12] I. M. Isaacs, W. M. Kantor and N. Spaltenstein, On the probability that a group element *is p-singular, J. Algebra* 176(1995) 139-181.

[13] G. I. Lehrer, Rational tori, semsimple orbits and the topology of hyperplane complements, *Comment. Math. Helv.* 67(1992) 226-251.

[14] F. Lübeck, A. C. Niemeyer and C. E. Praeger, Finding involutions in finite Lie type groups of odd charachteristic, *J. Algebra* 321(2009) 3397-3417.

[15] A. C. Niemeyer, T. Popiel and C. E. Praeger, Finding involution whit eigenspaces of given dimensions in finite classical groups, *J. Algebra* 324(2010) 1016-1043.

[16] A. C. Niemeyer and C. E. Praeger, Estimating propotions of elemnts in finite simple groups of Lie type, *J. Algebra* 324(2010) 122-154.

[17] C.W. Parker and R. A. Wilson, Recognising simplicity of black-box groups by constructing involution and their centralisers, *J. Algebra* 324(2010) 885-915.

[18] C. E. Praeger and Á. Seress, Probabilistic generation of finite classical groups in odd characteristic by involutions, *J. group Theory,* in press dio: 10.1515/JGT. 2010.061.

[19] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type, preprint (2010). arXiv:1005.1858vl.

مرجع:

Asia Pacific Mathematics Newsletter, July 2011, Vol. 1, No. 3, P. 7 - P. 10.

مترجم: محمدرضا درفشه
استاد دانشگاه تهران