فرهنگ و اندیشهٔ ریاضی

سال ۴۲، شمارهٔ ۷۲ (بهار و تابستان ۱۴۰۲) صص. ۱۱۱ تا ۱۲۷

تفاضل متقارن، عدد اصلی، و احتمال

علی پارسیان✉، زهرا پارسیان

چکیده. در بیشتر متون ریاضی، به عمل تفاضل متقارن و ویژگی‌های آن کمتر توجه شده است. در این مقاله، نخست برخی ویژگی‌های اساسی این عمل را اثبات و سپس فرمولی بیان می‌کنیم که در آن عدد اصلی مجموعه‌ای متشکل از ترکیب تفاضل متقارن تعداد متناهی مجموعه برحسب عدد اصلی مجموعه‌های تشکیل‌دهنده تعیین می‌شود. همچنین، فرمولی برای محاسبهٔ احتمال وقوع پیشامدی متشکل از ترکیب تفاضل متقارن تعداد متناهی پیشامد برحسب احتمال پیشامدهای تشکیل‌دهنده ارائه می‌دهیم. سرانجام، مقاله را با اشاره به کاربردی از این روابط در نظریهٔ رمز به پایان می‌بریم.

۱ مقدمه

فرض کنید $S \neq \emptyset$ مجموعهٔ مرجع و $\mathbb{P}(S)$ مجموعهٔ توانی آن باشد. چهار عمل اصلی روی اعضای $\mathbb{P}(S)$ عبارت‌اند از اجتماع، اشتراک، تفاضل، و متمم نسبت به S. عمل دیگری موسوم به تفاضل متقارن نیز وجود دارد که معمولاً، در کتاب‌های مبانی ریاضیات آن‌چنان که باید مانند چهار عمل اصلی دیگر پرداخته نمی‌شود. مثلاً در [۲] از تفاضل متقارن دو مجموعه سخنی به میان نیامده است. کتاب [۷] اشارهٔ مختصری به تعریف و برخی از ویژگی‌های آن دارد. در کتاب‌های [۵] و [۳] نیز، مانند برخی از کتاب‌های تخصصی ریاضیات، به تفاضل متقارن و ویژگی‌های آن فقط در تمرین‌ها پرداخته شده است. عمدهٔ مباحثی که در متون متداول جبری دربارهٔ عملگر تفاضل متقارن، $\triangle$، مطرح می‌شود مربوط به آن دسته از ساختارهای ریاضی است که $\triangle$ به‌عنوان یک عمل دوتایی در آن‌ها حضور دارد. برخی گروه‌های بولی و حلقه‌های بولی نمونه‌هایی از این ساختارها هستند [۱۵].

موضوع برخی از مقالات، مانند [۸، ۱۶]، اثبات ویژگی شرکت‌پذیری $\triangle$ است. تفاضل متقارن

عبارات و کلمات کلیدی: عدد اصلی، تفاضل متقارن، احتمال، جایگشت، اصل شمول و عدم شمول، رمزگذاری

نوع مقاله: پژوهشی؛ تاریخ دریافت: ۱۴۰۱/۴/۱؛ تاریخ پذیرش: ۱۴۰۱/۹/۸

doi: 10.30504/mct.2022.1300.1907

به برخی از نظریه‌های ریاضی نیز راه یافته است. مثلاً، در [۹] با استفاده از فنون نظریهٔ معادلات تابعی و نظریهٔ شبکه‌ها برخی الگوهای تفاضل متقارن برای مجموعه‌های فازی مطالعه شده است. در [۱۹] با استفاده از مباحث گوناگون ریاضیات، ازجمله بلوک‌ها، ماتریس‌های وقوع، ابرصفحه‌ها، و ماتریس‌های آدامار موضوع وجود یا عدم وجود ویژگی تفاضل متقارن در طرح‌های بلوکی و مجموعه‌های تفاضلی بررسی شده است. در [۱۴] روش محاسبهٔ تفاضل متقارن دو ناحیه از صفحه، که با خم‌های (ساده، بسته و جهت‌دار) چندضلعی و مرتبط با مرزهای وابستهٔ خود، تعریف شده‌اند بررسی شده است، و خروجی به شکل خم‌های چندضلعی ارائه شده است.

هدف اصلی مقالهٔ حاضر، که ترکیبی از مباحث جبری و احتمالاتی است، استفاده از مفهوم تفاضل متقارن در محاسبهٔ عدد اصلی دو مجموعهٔ خاص، و به‌دنبال آن، محاسبهٔ احتمال دو پیشامد خاص است. ویژگی این دو مجموعه، یا دو پیشامد، آن است که محاسبهٔ عدد اصلی، یا احتمال آن‌ها، بدون استفاده از این نماد با محاسبات پیچیده همراه است [۱۱، ۱۲]. مجموعهٔ (پیشامد) مورد بحث از ترکیب تفاضل متقارن تعداد متناهی مجموعه (پیشامد) به دست آمده است. در پایان، کاربردی از نتایج حاصل را در نظریهٔ رمز می‌آوریم.

۲ عدد اصلی برخی مجموعه‌های خاص

زیرمجموعه‌های A_1، ...، A_n از مجموعهٔ مرجع S را در نظر می‌گیریم. اصل شمول و عدم شمول فرمولی برای عدد اصلیِ زیرمجموعه‌ای از S که اعضای آن دست‌کم به یکی از زیرمجموعه‌های متناهی A_1، ...، A_n تعلق دارند به دست می‌دهد [۶]. در این بخش، به تعریف و نمایش دو مجموعه، که هر دو ترکیبی از مجموعه‌های A_1، ...، A_nاند، می‌پردازیم و فرمول‌هایی شبیه به فرمول اصل شمول و عدم شمول برای عدد اصلیِ آن‌ها بیان می‌کنیم. این دو مجموعه عبارت‌اند از

(الف) مجموعهٔ اعضایی از S که فقط به تعدادی فرد از زیرمجموعه‌های A_1، ...، A_n تعلق دارند؛

(ب) مجموعهٔ اعضایی از S که فقط به تعدادی زوج از زیرمجموعه‌های A_1، ...، A_n تعلق دارند.

مجموعه‌های یادشده در (الف) و (ب) بالا را به‌ترتیب با O_n و E_n نمایش می‌دهیم.

تعریف ۱.۲. فرض کنید $S \neq \emptyset$ مجموعهٔ مرجع و A_1، A_2، ...، A_n زیرمجموعه‌هایی از آن باشند. تفاضل متقارن این زیرمجموعه‌ها چنین تعریف می‌شود

$$A_1 \triangle A_2 \triangle \cdots \triangle A_n = \begin{cases} (A_1 - A_2) \cup (A_2 - A_1) & n = 2 \\ (A_1 \triangle A_2 \triangle \cdots \triangle A_{n-1}) \triangle A_n & n > 2 \end{cases}$$

در قضیهٔ زیر O_n و E_n را به کمک $\triangle$ توصیف می‌کنیم.

قضیه ۲.۲. فرض کنید $A_1, \ldots, A_n \subseteq S$. دراین‌صورت اعضای $A_1 \triangle A_2 \triangle \cdots \triangle A_n$ دقیقاً اعضایی از Sاند که به تعدادی فرد از زیرمجموعه‌های A_1، A_2، ...، A_n تعلق دارند، و اعضای متمم آن نسبت به S دقیقاً اعضایی از Sاند که به تعدادی زوج از زیرمجموعه‌های A_1، A_2، ...، A_n تعلق دارند. به‌عبارت‌دیگر،

$$O_n = A_1 \triangle A_2 \triangle \cdots \triangle A_n, \tag{۱.۲}$$

$$E_n = S - (A_1 \triangle A_2 \triangle \cdots \triangle A_n). \tag{۲.۲}$$

اثبات. کافی است (۱.۲) را به استقراء روی n ثابت کنیم. در حالت $n = 1$ حکم بدیهی است. اگر $n = 2$، آنگاه از فرمول $A_1 \triangle A_2 = (A_1 - A_2) \cup (A_2 - A_1)$ نتیجه می‌شود که $A_1 \triangle A_2$ دقیقاً متشکل از اعضایی از S است که از بین دو مجموعهٔ A_1 و A_2 فقط به یکی از آن‌ها تعلق دارند، بنابراین $O_2 = A_1 \triangle A_2$. فرض می‌کنیم که حکم برای هر $n = k$ درست باشد. از برابری

$$A_1 \triangle A_2 \triangle \cdots \triangle A_k \triangle A_{k+1} = (A_1 \triangle A_2 \triangle \cdots \triangle A_k) \triangle A_{k+1}$$

و آزمون استقراء نتیجه می‌شود که $A_1 \triangle A_2 \triangle \cdots \triangle A_k \triangle A_{k+1}$ متشکل از اعضایی از S است که از بین دو مجموعهٔ $A_1 \triangle A_2 \triangle \cdots \triangle A_k$ و A_{k+1} دقیقاً به یکی از آن‌ها تعلق دارند. بنابراین با توجه به آزمون و فرض استقراء، $A_1 \triangle A_2 \triangle \cdots \triangle A_k \triangle A_{k+1}$ متشکل از اعضایی از S است که به تعدادی فرد از A_1، A_2، ...، A_{k+1} تعلق دارند، و بنابراین به دست می‌آید $O_{k+1} = A_1 \triangle A_2 \triangle \cdots \triangle A_{k+1}$. □

تعریف ۳.۲. مجموعهٔ جایگشت‌های مجموعهٔ $L = \{1, 2, \ldots, n\}$ را با $\mathrm{Per}(L)$ نشان می‌دهیم.

نتیجه‌ای از قضیهٔ ۲.۲ چنین است.

نتیجه ۴.۲. اگر $A_1, \ldots, A_n \subseteq S$ و $\sigma \in \mathrm{Per}(L)$ آنگاه

$$A_{\sigma(1)} \triangle A_{\sigma(2)} \triangle \cdots \triangle A_{\sigma(n)} = A_1 \triangle A_2 \triangle \cdots \triangle A_n.$$

قضیه ۵.۲. اگر $A_1, \dots, A_n \subseteq S$، $1 < k_1 < k_2 < \cdots < k_m < n$، $\sigma \in \mathrm{Per}(L)$، و $X = A_1 \triangle A_2 \triangle \cdots \triangle A_n$،

$$Y = (A_{\sigma(1)} \triangle \cdots \triangle A_{\sigma(k_1)}) \triangle (A_{\sigma(k_1+1)} \triangle \cdots \triangle A_{\sigma(k_2)}) \triangle \cdots \triangle (A_{\sigma(k_m+1)} \triangle \cdots \triangle A_{\sigma(n)})$$

آنگاه $X = Y$.

اثبات. بدون کاستن از کلیت، و بنابر قضیهٔ ۲.۲ فرض می‌کنیم A_iها متمایزند. تعریف می‌کنیم

$$\begin{aligned} B_{\sigma(1)} &= A_{\sigma(1)} \triangle \cdots \triangle A_{\sigma(k_1)} \\ B_{\sigma(k_1+1)} &= A_{\sigma(k_1+1)} \triangle \cdots \triangle A_{\sigma(k_2)} \\ &\vdots \qquad\qquad\qquad \vdots \\ B_{\sigma(k_m+1)} &= A_{\sigma(k_m+1)} \triangle \cdots \triangle A_{\sigma(n)}. \end{aligned}$$

بنابر قضیهٔ ۲.۲، مجموعهٔ $Y = B_{\sigma(1)} \triangle B_{\sigma(k_1+1)} \triangle \cdots \triangle B_{\sigma(k_m+1)}$ از همهٔ اعضایی از S تشکیل شده است که هریک به تعدادی فرد از مجموعه‌های $B_{\sigma(1)}$، $B_{\sigma(k_1+1)}$، ...، $B_{\sigma(k_m+1)}$ تعلق دارند. ازسوی‌دیگر، بنابر همان قضیه، هریک از این مجموعه‌ها نیز از اعضایی از S تشکیل شده است که هریک به تعدادی فرد از مجموعه‌های A_i تعلق دارند. چون $\sigma \in \mathrm{Per}(L)$ و A_iها متمایزند، Y از اعضایی از S تشکیل شده است که هریک به تعدادی فرد از A_iها تعلق دارند، بنابراین $Y \subseteq X$. اگر $X \not\subseteq Y$ آنگاه عضوی از X وجود دارد که به تعدادی زوج از مجموعه‌های $B_{\sigma(1)}$، $B_{\sigma(k_1+1)}$، ...، $B_{\sigma(k_m+1)}$ تعلق دارد. چون، هریک از این مجموعه‌ها نیز، از اعضایی از S تشکیل شده است که هریک به تعدادی فرد از مجموعه‌های A_i تعلق دارند، پس عضوی از X وجود دارد که به تعدادی زوج از A_iها متعلق است. این نتیجه با قضیهٔ ۲.۲ تناقض دارد. □

نتیجه ۶.۲. عمل $\triangle$ ویژگی شرکت‌پذیری دارد.

اثبات. کافی است در قضیهٔ ۵.۲ بگذاریم $n = 3$ و $k_1 = 2$ و $\sigma \in \mathrm{Per}(L)$ را به‌گونه‌ای در نظر بگیریم که $\sigma(1) = 2$، $\sigma(2) = 3$، و $\sigma(3) = 1$. دراین‌صورت، طبق قضیهٔ ۵.۲ داریم

$$Y = (A_{\sigma(1)} \triangle A_{\sigma(2)}) \triangle A_{\sigma(3)}, \quad X = A_1 \triangle A_2 \triangle A_3.$$

با استفاده از ویژگی جابه‌جایی $\triangle$، که از تعریف ۱.۲ نتیجه می‌شود، و قضیهٔ ۵.۲ داریم

$$\begin{aligned} A_1\triangle(A_2\triangle A_3) &= (A_2\triangle A_3)\triangle A_1 \\ &= (A_{\sigma(1)}\triangle A_{\sigma(2)})\triangle A_{\sigma(3)} \\ &= A_1\triangle A_2\triangle A_3 = (A_1\triangle A_2)\triangle A_3. \end{aligned}$$

□

قضیه ۷.۲. فرض کنید $B, A_1, \ldots, A_n \subseteq S$ دراین‌صورت

$$(A_1\triangle A_2\triangle\cdots\triangle A_n)\cap B = (A_1\cap B)\triangle(A_2\cap B)\triangle\cdots\triangle(A_n\cap B), \qquad (۳.۲)$$

$$B\cap(A_1\triangle A_2\triangle\cdots\triangle A_n) = (B\cap A_1)\triangle(B\cap A_2)\triangle\cdots\triangle(B\cap A_n). \qquad (۴.۲)$$

اثبات. نخست رابطهٔ (۳.۲) را به استقراء روی n ثابت می‌کنیم. به‌ازای $n = 1$ حکم بدیهی است. فرض می‌کنیم $n = 2$ و درستی $B\cap(A_1\triangle A_2) = (B\cap A_1)\triangle(B\cap A_2)$ را ثابت می‌کنیم. داریم

$$\begin{aligned} x\in B\cap(A_1\triangle A_2) \iff & (x\in B\wedge x\in A_1\triangle A_2) \\ \iff & (x\in B\wedge(x\in A_1\wedge x\notin A_2)) \\ & \vee(x\in B\wedge(x\notin A_1\wedge x\in A_2)) \\ \iff & ((x\in B\wedge x\in A_1)\wedge(x\in B\wedge x\notin A_2)) \\ & \vee((x\in B\wedge x\notin A_1)\wedge(x\in B\wedge x\in A_2)) \\ \iff & (x\in(B\cap A_1)\wedge x\notin(B\cap A_2)) \\ & \vee(x\notin(B\cap A_1)\wedge x\in(B\cap A_2)) \\ \iff & x\in(B\cap A_1)\triangle(B\cap A_2) \end{aligned}$$

بنابراین، حکم به‌ازای $n = 2$ برقرار است. فرض می‌کنیم حکم به‌ازای $n = k$ نیز برقرار باشد و

$$B\cap(A_1\triangle A_2\triangle\cdots\triangle A_k) = (B\cap A_1)\triangle(B\cap A_2)\triangle\cdots\triangle(B\cap A_k)$$

برای $n = k + ۱$، با استفاده از تعریف ۱.۲ و آزمون و فرض استقراء داریم

$$\begin{aligned}
&B \cap (A_۱ \triangle A_۲ \triangle \cdots \triangle A_k \triangle A_{k+۱}) \\
&\quad = B \cap ((A_۱ \triangle A_۲ \triangle \cdots \triangle A_k) \triangle A_{k+۱}) \\
&\quad = (B \cap (A_۱ \triangle A_۲ \triangle \cdots \triangle A_k)) \triangle (B \cap A_{k+۱}) \\
&\quad = ((B \cap A_۱) \triangle (B \cap A_۲) \triangle \cdots \triangle (B \cap A_k)) \triangle (B \cap A_{k+۱}) \\
&\quad = (B \cap A_۱) \triangle (B \cap A_۲) \triangle \cdots \triangle (B \cap A_k) \triangle (B \cap A_{k+۱})
\end{aligned}$$

و اثبات (۳.۲) به اتمام می‌رسد. اثبات (۴.۲) به‌طور مشابه انجام می‌شود. □

در ادامه، فرمول‌هایی برای اعداد اصلی O_n و E_n به‌دست می‌آوریم. این فرمول‌ها شباهت زیادی به فرمول اصل شمول و عدم شمول دارند.

قضیه ۸.۲ (اصل شمول و عدم شمول، [۶]). اگر $A_۱, \ldots, A_n \subseteq S$ زیرمجموعه‌های متناهی از S باشند و $A = \cup_{i=۱}^{i=n} A_i$، آنگاه با فرض

$$\begin{aligned}
&c_i = |A_i|, \quad c_{ij} = |A_i \cap A_j|, \quad c_{ijk} = |A_i \cap A_j \cap A_k|, \ \ldots \\
&C_۱^n = \sum_i c_i, \quad C_۲^n = \sum_{i<j} c_{ij}, \quad C_۳^n = \sum_{i<j<k} c_{ijk}, \ \ldots
\end{aligned}$$

عدد اصلی A چنین است

$$|A| = \sum_{\nu=۱}^{n} (-۱)^{\nu-۱} C_\nu^n$$

تعریف ۹.۲. عضو $i \in L$ را یک نقطهٔ ثابت $f \in \mathrm{Per}(L)$ می‌نامند هرگاه $f(i) = i$. مجموعهٔ همه اعضای $\mathrm{Per}(L)$ را که حداقل یک نقطهٔ ثابت دارند با $\mathrm{Fix}(L)$ نشان می‌دهیم.

نتیجه ۱۰.۲. عدد اصلیِ مجموعهٔ $\mathrm{Fix}(L)$ برابر است با

$$|\mathrm{Fix}(L)| = n! \sum_{\nu=۱}^{n} \frac{(-۱)^{\nu+۱}}{\nu!}$$

اثبات. برای $۱ \le i \le n$ تعریف می‌کنیم

$$A_i = \{f \in \mathrm{Per}(L) : f(i) = i\}.$$

طبق نمادهای قضیهٔ ۸.۲ داریم

$$c_i = (n-۱)!, \quad c_{ij} = (n-۲)!, \quad c_{ijk} = (n-۳)!, \ \ldots.$$

چون تعداد راه‌های انتخاب m شیء مختلف از بین n شیء مختلف برابر است با $\binom{n}{m}$ پس داریم

$$\begin{aligned}
C_۱^n &= \binom{n}{۱}(n-۱)! = n(n-۱)! = n!,\\
C_۲^n &= \binom{n}{۲}(n-۲)! = \frac{n(n-۱)}{۲!}(n-۲)! = \frac{n!}{۲!},\\
C_۳^n &= \binom{n}{۳}(n-۳)! = \frac{n(n-۱)(n-۲)}{۳!}(n-۳)! = \frac{n!}{۳!},
\end{aligned}$$

و غیره. چون $\mathrm{Fix}(L) = A_۱ \cup \cdots \cup A_n$، بنابراین با استفاده از قضیهٔ ۸.۲ داریم

$$\begin{aligned}
|\mathrm{Fix}(L)| &= C_۱^n - C_۲^n + \cdots + (-۱)^{n-۱} C_n^n\\
&= n! - \frac{n!}{۲!} + \cdots + (-۱)^{n-۱}\frac{n!}{n!}\\
&= n!\left(۱ - \frac{۱}{۲!} + \cdots + \frac{(-۱)^{n-۱}}{n!}\right) = n!\sum_{\nu=۱}^{n}\frac{(-۱)^{\nu+۱}}{\nu!}
\end{aligned}$$

□

قضیه ۱۱.۲. فرض می‌کنیم $A_۱, \ldots, A_n \subseteq S$ زیرمجموعه‌های متناهی از S باشند. دراین‌صورت با نمادهای قضیهٔ ۸.۲ داریم

$$|O_n| = \sum_{\nu=۱}^{n}(-۲)^{\nu-۱} C_\nu^n, \tag{۵.۲}$$

$$|E_n| = |S| - \sum_{\nu=۱}^{n}(-۲)^{\nu-۱} C_\nu^n. \tag{۶.۲}$$

اثبات. رابطهٔ (۵.۲) را ثابت می‌کنیم. بنابر قضیهٔ ۲.۲، کافی است رابطهٔ

$$|A_۱ \triangle A_۲ \triangle \cdots \triangle A_n| = \sum_{\nu=۱}^{n}(-۲)^{\nu-۱} C_\nu^n$$

را ثابت کنیم. در حالت $n = ۱$ حکم بدیهی است. اگر $n = ۲$ آنگاه

$$\begin{aligned}|A_۱ \triangle A_۲| &= |A_۱ \cup A_۲| - |A_۲ \cap A_۱| \\ &= |A_۱| + |A_۲| - ۲|A_۱ \cap A_۲| \\ &= c_۱ + c_۲ - ۲c_{۱۲} = C_۱^۲ - ۲C_۲^۲ = \sum_{\nu=۱}^{۲} (-۲)^{\nu-۱} C_\nu^۲,\end{aligned}$$

بنابراین حکم برای $n = ۲$ نیز برقرار است. فرض می‌کنیم حکم برای $n = k$ برقرار است،

$$|A_۱ \triangle A_۲ \triangle \cdots \triangle A_k| = \sum_{\nu=۱}^{k} (-۲)^{\nu-۱} C_\nu^k$$

برای $۱ \le i \le k$ تعریف می‌کنیم $B_i = A_i \cap A_{k+۱}$، دراین‌صورت

$$\begin{aligned}|B_i| &= |A_i \cap A_{k+۱}| = c_{i(k+۱)}, \\ |B_i \cap B_j| &= |A_i \cap A_j \cap A_{k+۱}| = c_{ij(k+۱)}, \dots .\end{aligned}$$

بنابر تعریف ۱.۲، آزمون استقراء، و قضیهٔ ۷.۲ داریم

$$\begin{aligned}|A_۱ \triangle A_۲ \triangle \cdots \triangle A_{k+۱}| &= |(A_۱ \triangle A_۲ \triangle \cdots \triangle A_k) \triangle A_{k+۱}| \\ &= |A_۱ \triangle A_۲ \triangle \cdots \triangle A_k| + |A_{k+۱}| \\ &\quad - ۲|(A_۱ \triangle A_۲ \triangle \cdots \triangle A_k) \cap A_{k+۱}| \\ &= |A_۱ \triangle A_۲ \triangle \cdots \triangle A_k| + |A_{k+۱}| \\ &\quad - ۲|(A_۱ \cap A_{k+۱}) \triangle \cdots \triangle (A_k \cap A_{k+۱}| \\ &= |A_۱ \triangle A_۲ \triangle \cdots \triangle A_k| + |A_{k+۱}| - ۲|B_۱ \triangle \cdots \triangle B_k|. \qquad (۷.۲)\end{aligned}$$

بنابر فرض استقراء داریم

$$|B_۱ \triangle \cdots \triangle B_k| = \sum_{\mu=۱}^{k} (-۲)^{\mu-۱} D_\mu^k \qquad (۸.۲)$$

که در آن

$$D_1^k = \sum_{1\le i\le k} |B_i| = \sum_{1\le i\le k} c_{i(k+1)},$$
$$D_2^k = \sum_{1\le i<j\le k} |B_i\cap B_j| = \sum_{1\le i<j\le k} c_{ij(k+1)},$$
$$D_3^k = \sum_{1\le i<j<\ell<\le k} |B_i\cap B_j\cap B_\ell| = \sum_{1\le i<j<\ell<\le k} c_{ij\ell(k+1)},$$

و غیره. بنابراین از رابطه‌های (۷.۲) و (۸.۲) داریم

$$\begin{aligned}|A_1\triangle A_2\triangle\cdots\triangle A_{k+1}| &= \sum_{\nu=1}^{k}(-2)^{\nu-1}C_\nu^k + c_{k+1} - 2\sum_{\mu=1}^{k}(-2)^{\mu-1}D_\mu^k\\
&= (C_1^k + c_{k+1}) - 2(C_2^k + D_1^k) + 4(C_3^k + D_2^k) - \cdots\\
&\quad + (-2)^{k-1}(C_k^k + D_{k-1}^k) + (-2)^k D_k^k\\
&= C_1^{k+1} - 2C_2^{k+1} + 4C_3^{k+1} - \cdots + (-2)^{k-1}C_k^{k+1} + (-2)^k C_{k+1}^{k+1}\\
&= \sum_{\nu=1}^{k+1}(-2)^{\nu-1}C_\nu^{k+1}\end{aligned}$$

و درنتیجه اثبات به انجام می‌رسد. □

با استفاده از قضیهٔ ۱۱.۲ و استدلالی مشابه نتیجهٔ ۱۰.۲ می‌توان عدد اصلیِ مجموعهٔ اعضایی از $\mathrm{Per}(L)$ را که تعدادی فرد نقطهٔ ثابت دارند به دست آورد.

نتیجه ۱۲.۲. عدد اصلیِ مجموعهٔ اعضایی از $\mathrm{Per}(L)$ که تعدادی فرد نقطهٔ ثابت دارند برابر است با $n!\sum_{\nu=1}^{n}\frac{(-2)^{\nu-1}}{\nu!}$.

اثبات. به‌ازای $1\le i\le n$ تعریف می‌کنیم

$$A_i = \{f\in \mathrm{Per}(L) : f(i) = i\}.$$

بدیهی است که مجموعهٔ اعضایی از $\mathrm{Per}(L)$ که تعدادی فرد نقطهٔ ثابت دارند برابر است با $A_1\triangle A_2\triangle\ldots\triangle A_n$، بنابراین مانند نتیجهٔ ۱۰.۲ داریم

$$c_i = (n-1)!,\quad c_{ij} = (n-2)!,\quad c_{ijk} = (n-3)!,\ \ldots.$$

و به‌همین‌ترتیب

$$C_۱^n = n!, \quad C_۲^n = \frac{n!}{۲!}, \quad C_۳^n = \frac{n!}{۳!}, \ \ldots.$$

درنتیجه طبق قضیهٔ ۱۱.۲ داریم

$$\begin{aligned} |A_۱ \triangle A_۲ \triangle \cdots \triangle A_n| &= \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} C_\nu^n \\ &= \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} \frac{n!}{\nu!} = n! \sum_{\nu=۱}^{n} \frac{(-۲)^{\nu-۱}}{\nu!}, \end{aligned}$$

و اثبات کامل است. □

۳ تفاضل متقارن در نظریهٔ احتمالات

در نظریهٔ احتمالات منظور از آزمایش عملی است که نتیجه‌اش را با قاطعیت نتوان پیش‌بینی کرد. مجموعهٔ تمام نتایجی که یک آزمایش ممکن است داشته باشد فضای نمونهٔ آن آزمایش می‌نامند.

تعریف ۱.۳. [۱۳]: فرض می‌کنیم S فضای نمونهٔ یک آزمایش باشد. یک سیگما جبر (سیگما میدان) روی S عبارت است از زیرمجموعهٔ Σ از $\mathbb{P}(S)$ که در شرایط زیر صدق کند

(الف) $S \in \Sigma$؛

(ب) اگر $A \in \Sigma$ آنگاه $S - A \in \Sigma$؛

(ج) اجتماع هر دنباله از اعضای Σ متعلق به Σ باشد.

هر عضو Σ را یک پیشامد آزمایش می‌نامند. یک پیشامد وقتی رخ می‌دهد که نتیجهٔ آزمایش یکی از اعضایش باشد. دو پیشامد را ناسازگار نامند هرگاه با هم رخ ندهند. روشن است که $\mathbb{P}(S)$ خود یک سیگما جبر روی S است.

تعریف ۲.۳ ([۱۰]). تابع $P : \mathbb{P}(S) \to [۰, ۱]$ را که در دو رابطهٔ زیر صدق می‌کند، تابع احتمال آزمایش با فضای نمونهٔ S می‌نامیم.

(الف) برای فضای نمونهٔ S داشته باشیم $P(S) = ۱$؛

(ب) اگر $\{A_i\}_{i \in N}$ دنباله‌ای از پیشامدهای دوبه‌دو ناسازگار باشد، آنگاه

$$P(\cup_{i=۱}^{\infty} A_i) = \sum_{i=۱}^{\infty} P(A_i).$$

سه گزارهٔ زیر نتایج تعریف تابع احتمال‌اند [۱۷].

(۱) برای هر دو پیشامد $A_۱$ و $A_۲$ داریم

$$P(A_۱ \cup A_۲) = P(A_۱) + P(A_۲) - P(A_۱ \cap A_۲).$$

(۲) اگر $A_۱ \subseteq A_۲$ آنگاه $P(A_۱) \leq P(A_۲)$.

(۳) $P(\emptyset) = ۰$.

مشابه آنچه بیان شد، پیشامدی از S را که هر عضوش فقط به تعدادی فرد از پیشامدهای $A_۱$، $A_۲$، ...، A_n تعلق دارد با O_n، و پیشامدی از S را که هر عضوش فقط به تعدادی زوج از پیشامدهای $A_۱$، $A_۲$، ...، A_n تعلق دارد با E_n نمایش می‌دهیم.

۱.۳ احتمال برخی پیشامدهای خاص

در اینجا، فرمول‌هایی برای $P(O_n)$ و $P(E_n)$ می‌یابیم. ابتدا فرض می‌کنیم S فضای نمونهٔ یک آزمایش و $A_۱$، ...، A_n پیشامدهای مستقل و احتمال رخ‌دادن هریک r باشد. احتمال رخ‌دادن k پیشامد از بین پیشامدهای $A_۱$، ...، A_n برابر است با $\binom{n}{k} r^k s^{n-k}$ که در آن $s = ۱ - r$ و $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. مجموعهٔ اعداد فرد واقع در بازهٔ $[۱, n]$ را با $o(n)$ نمایش می‌دهیم. درنتیجه، احتمال رخ‌دادن O_n برابر است با $\sum_{k \in o(n)} \binom{n}{k} r^k s^{n-k}$. این مجموع، همان مجموع جمله‌های بسط دوجمله‌ای $(r+s)^n$ است که در آن‌ها k فرد است. بنابراین، مقدار آن با نصفِ مقدار تفاضل بسط‌های دوجمله‌ای‌های $(r+s)^n$ و $(s-r)^n$ برابر است.

قضیه ۳.۳. اگر پیشامدهای $A_۱$، ...، A_n مستقل و احتمال رخ‌دادن هریک r باشد، آنگاه

$$P(O_n) = \frac{۱}{۲}[۱ - (۱ - ۲r)^n], \qquad P(E_n) = \frac{۱}{۲}[۱ + (۱ - ۲r)^n],$$
$$\lim_{n\to\infty} P(O_n) = \lim_{n\to\infty} P(E_n) = \frac{۱}{۲}.$$

اکنون حالت کلی را در نظر می‌گیریم. با برهانی شبیه به برهان قضیهٔ ۱۱.۲ و با تبدیل $|\cdot|$ به P، و C به F می‌توان فرمولی برای احتمال رخ‌دادن تعدادی فرد از A_iها استخراج کرد.

قضیه ۴.۳. فرض می‌کنیم S متناهی باشد و $A_۱, \dots, A_n \subseteq S$. همچنین،

$$P_i = P(A_i), \quad P_{ij} = P(A_i \cap A_j), \quad P_{ijk} = P(A_i \cap A_j \cap A_k), \dots$$
$$F_۱^n = \sum_i P_i, \quad F_۲^n = \sum_{i<j} P_{ij}, \quad F_۳^n = \sum_{i<j<k} P_{ijk}, \dots.$$

دراین‌صورت

$$P(O_n) = \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} F_\nu^n, \quad P(E_n) = ۱ - \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} F_\nu^n.$$

ملاحظه ۵.۳. درحالتی‌که پیشامدهای $A_۱$، ...، A_n مستقل و احتمال رخ‌دادن هریک r باشد، فرمول‌های قضیهٔ ۳.۳ از فرمول‌های قضیهٔ ۴.۳ نتیجه می‌شوند. می‌دانیم

$$P_i = r, \quad P_{ij} = r^۲, \quad P_{ijk} = r^۳, \dots.$$

درنتیجه

$$F_۱^n = \binom{n}{۱} r, \quad F_۲^n = \binom{n}{۲} r^۲, \quad F_۳^n = \binom{n}{۳} r^۳, \dots, \quad F_\nu^n = \binom{n}{\nu} r^\nu.$$

بنابراین

$$\begin{aligned} P(O_n) = \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} F_\nu^n &= \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} \binom{n}{\nu} r^\nu \\ &= -\frac{۱}{۲}[-۱ + ۱ + \sum_{\nu=۱}^{n} \binom{n}{\nu} (-۲r)^\nu] \\ &= \frac{۱}{۲}[۱ - (۱ - ۲r)^n]. \end{aligned}$$

قضیه ۶.۳. به‌ازای هر $۱ \le i \le n$ تعریف می‌کنیم

$$A_i = \{f \in \mathrm{Per}(L) : f(i) = i\}.$$

دراین‌صورت

$$P(O_n) = \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} \frac{۱}{\nu!}, \qquad P(E_n) = ۱ - \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} \frac{۱}{\nu!}.$$

اثبات. بنابر قضیهٔ ۴.۳ داریم

$$P_i = \frac{|A_i|}{|S|} = \frac{(n-۱)!}{n!} = \frac{۱}{n},$$
$$P_{ij} = \frac{|A_i \cap A_j|}{|S|} = \frac{(n-۲)!}{n!} = \frac{۱}{n(n-۱)},$$
$$P_{ijk} = \frac{|A_i \cap A_j \cap A_k|}{|S|} = \frac{(n-۳)!}{n!} = \frac{۱}{n(n-۱)(n-۲)},$$

و غیره. همچنین

$$F_۱^n = \binom{n}{۱} P_i = ۱, \quad F_۲^n = \binom{n}{۲} P_{ij} = \frac{۱}{۲!}, \quad F_۳^n = \binom{n}{۳} P_{ijk} = \frac{۱}{۳!}, \ldots.$$

درنتیجه بنابر همان قضیه داریم $P(O_n) = \sum_{\nu=۱}^{n} (-۲)^{\nu-۱} \frac{۱}{\nu!}$ و اثبات کامل می‌شود. □

قضیه ۷.۳. اگر $L = \{۱, ۲, \ldots, n\}$ و برای $۱ \le i \le n$ تعریف کنیم

$$A_i = \{f \in \mathrm{Per}(L) : f(i) = i\},$$

آنگاه $P(O_n)$ و $P(E_n)$ با حداکثر خطای $\frac{۲^n}{(n+۱)!}$، به‌ترتیب، با $\frac{۱-e^{-۲}}{۲}$ و $\frac{۱+e^{-۲}}{۲}$ برابر است.

اثبات. حاصل $P(O_n)$ با n جملهٔ اول بسط تیلر تابع $\frac{۱-e^x}{۲}$ در $x = -۲$ برابر است. در چنین سری متناوبی، که قدرمطلق جمله‌ها رفته‌رفته کاهش می‌یابد، قدرمطلق خطایی که در اثر برش ایجاد می‌شود از قدرمطلق اولین جملهٔ صرف‌نظرشده کوچک‌تر است [۱]. ازاین‌رو،

$$\left| P(E_n) - \frac{۱+e^{-۲}}{۲} \right| = \left| (۱ - P(O_n)) - \frac{۱+e^{-۲}}{۲} \right|$$
$$= \left| P(O_n) - \frac{۱-e^{-۲}}{۲} \right| < \frac{۲^n}{(n+۱)!}.$$

□

نتیجه ۸.۳. به‌ازای $L = \{۱, ۲, \ldots, n\}$ و $۱ \le i \le n$ تعریف می‌کنیم

$$A_i = \{f \in \mathrm{Per}(L) : f(i) = i\}.$$

دراین‌صورت $P(O_n)$ و $P(E_n)$ در برابری‌های زیر صدق می‌کنند.

$$\lim_{n\to\infty} P(O_n) = \frac{۱}{۲}(۱ - e^{-۲}), \qquad \lim_{n\to\infty} P(E_n) = \frac{۱}{۲}(۱ + e^{-۲}).$$

درادامه، تعریفی می‌آوریم.

تعریف ۹.۳ ([۶]). هر عضو $\mathrm{Per}(L)$ را که فاقد نقطهٔ ثابت باشد پریشی از L می‌نامیم. مجموعه همهٔ پریش‌های L را با $\mathrm{Der}(L)$ نشان می‌دهیم.

از اصل شمول و عدم شمول نتیجه می‌شود که احتمال اینکه عضوی از $\mathrm{Per}(L)$، که به‌تصادف انتخاب می‌شود، متعلق به $\mathrm{Der}(L)$ باشد برابر است با $P(\mathrm{Der}(L)) = \sum_{\nu=۰}^{n} \frac{(-۱)^{\nu}}{\nu!}$. زیرا از تعریف ۹.۲ نتیجه می‌شود که $\mathrm{Der}(L)$ مکمل $\mathrm{Fix}(L)$ نسبت به $\mathrm{Per}(L)$ است، بنابراین از نتیجهٔ ۱۰.۲ داریم

$$\begin{aligned}|\mathrm{Der}(L)| &= n! - n!\left(۱ - \frac{۱}{۲!} + \cdots + \frac{(-۱)^{n-۱}}{n!}\right) \\ &= n!\left(۱ - ۱ + \frac{۱}{۲!} - \cdots + \frac{(-۱)^{n-۱}}{n!}\right) = n!\sum_{\nu=۰}^{n}\frac{(-۱)^{\nu}}{\nu!}.\end{aligned}$$

درنتیجه

$$P(\mathrm{Der}(L)) = \frac{|\mathrm{Der}(L)|}{|\mathrm{Per}(L)|} = \sum_{\nu=۰}^{n}\frac{(-۱)^{\nu}}{\nu!}$$

با استفاده از بسط تیلرِ تابع e^{x} در نقطهٔ $x = -۱$ و استدلالی شبیه به قضیهٔ ۷.۳ داریم

$$\left|P(\mathrm{Der}(L)) - \frac{۱}{e}\right| < \frac{۱}{(n+۱)!}, \quad \lim_{n\to\infty} P(\mathrm{Der}(L)) = \frac{۱}{e}.$$

بنابراین با توجه به آنچه بیان شد و قضیهٔ ۷.۳ داریم

نتیجه ۱۰.۳. اگر $L = \{۱, ۲, \ldots, n\}$ و برای $۱ \le i \le n$ تعریف کنیم

$$A_i = \{f \in \mathrm{Per}(L) : f(i) = i\}$$

دراین‌صورت احتمال اینکه عضوی از $\mathrm{Per}(L)$، که به‌تصادف انتخاب می‌شود، متعلق به تعدادی زوج و ناصفر از A_iها باشد برابر است با

$$P(E_n - \mathrm{Der}(L)) = -\sum_{\nu=۱}^{n}\frac{۱}{\nu!}[(-۲)^{\nu-۱} + (-۱)^{\nu}].$$

همچنین

$$\left|P(E_n - \mathrm{Der}(L)) - [\frac{۱}{۲}(۱ + e^{-۲}) - \frac{۱}{e}]\right| < \frac{۲^{n}+۱}{(n+۱)!}.$$

۴ کاربردی در رمزگشایی

واژهٔ cryptography، که از ریشهٔ یونانی kryptós به معنی پوشیدگی و graphein به معنی نوشتن آمده است، نام علم و هنری است که تبادل پیام را برای همه بجز افراد معینی غیرقابل‌فهم می‌سازد. حیات این علم قرن‌ها به محیط‌های سیاسی و نظامی محدود بود که از آن برای استتار اطلاعات مبادله‌شده از طریق خطوط ارتباطی (امن یا ناامن) استفاده می‌کردند [۱۸].

یک رمز، دستگاهی است که با به‌کارگیری مجموعه‌ای از تبدیل‌ها روی الفبای پیام اصلی آن را به پیامی رمزی تبدیل می‌کند. تبدیل مورد استفاده، در هر لحظه توسط یک کلید که در همان لحظه به کار می‌رود، کنترل می‌شوند. امنیت پیام رمزی به میزان زیادی به سرّی ماندن کلید بستگی دارد. هدف رمزگشا یافتن کلید و شکستن رمز است. یکی از اولین دستگاه‌های رمزنگاری که تاکنون شناخته شده است رمز سزار است که توسط ژولیوس سزار در ۵۰ سال قبل از میلاد مورد استفاده قرار می‌گرفته است. در این رمز، حروف الفبا، سه واحد به سمت راست منتقل و سه حرف انتهایی نیز به سه حرف اول بازگردانده می‌شوند. البته، علت انتخاب عدد ۳ توسط سزار، به‌عنوان کلید دستگاه رمزیِ خود، مشخص نیست، زیرا او می‌توانست هر عدد صحیحی را انتخاب کند. برای زبان پیام به انگلیسی که در آن تعداد حروف الفبا ۲۶ است، ۲۵ کلید متمایز وجود دارد و یکی از آن‌ها هیچ اختفایی ایجاد نمی‌کند. بدیهی است پیامی که با استفاده از دستگاه رمزنگاری سزار رمزگذاری شود بسیار ناامن است. هر رمزی که با استفاده از یکی از این کلیدها انجام شود، رمز خطی نامیده می‌شود [۱۸].

رمز جانشینی رمزی است که کلید آن، مثلاً برای زبان انگلیسی، یک جایگشت روی ۲۶ حرف الفبا است. در این نوع رمزگذاری تعداد کلیدهای ممکن به $!۲۶ - ۱$ افزایش می‌یابد که عددی بزرگ‌تر از ۴×۱۰^{۲۶} است و به‌گونه‌ای مؤثّر تحلیل رمزی کامل را ناممکن می‌سازد. رمزهای خطی از نوع رمزهای جانشینی‌اند [۴].

برای رمزگشایی یک پیام رمزی که در زبان معینی نوشته شده و با استفاده از یک رمزِ جانشینی رمزگذاری شده است از توزیع فراوانی آماری یک حرف تنها که در آن زبان رخ می‌دهد استفاده می‌کنند. مقایسهٔ فراوانی توزیع حروف، حروف ابتدایی، انتهایی، ترکیبات دوحرفی، و سه‌حرفی از یک پیام رمزی با فراوانی‌های مشخص و معلوم در زبان مورد مکاتبه، از راهکارهای گشایش رمز است. این روش به‌طرز خاصی مؤثّر است، زیرا هر حرف پیام اصلی همواره با حرف مشابهی در پیام

رمزی داده‌شده نمایش داده می‌شود. به همین دلیل، کلیهٔ مشخصات زبانیِ پیامِ اصلی، در زبان مورد استفاده در پیام رمزی برقرار می‌ماند.

احتمال گشایش تصادفی رمز در رمزهای جانشینی بسیار کم است، زیرا در این حالت، رمزگشا باید برای پیامی که (مثلاً) به زبان انگلیسی است از بین (۱ − ۲۶!) گزینه یکی را انتخاب کند؛ پیشامدی که احتمال وقوع آن $P = \frac{۱}{۲۶!-۱}$ و مقدار تقریبی آن $۲٫۴۸ \times ۱۰^{-۲۷}$ است. اما اگر رمزگشا کلید را از بین جایگشت‌هایی جستجو کند که تعدادی فرد (زوج) حرف را ثابت نگه می‌دارند، این احتمال به‌طور چشمگیری افزایش می‌یابد. درحقیقت، قضیهٔ ۷.۳ نشان می‌دهد که این احتمال با حداکثر خطای $۶٫۱۷ \times ۱۰^{-۲۱} \approx \frac{۲^{۲۶}}{(۲۷)!} = \frac{۲^n}{(n+۱)!}$ به‌ترتیب برای جایگشت‌های با تعداد فرد و زوج حرفِ ثابت، با مقادیر تقریبی $\frac{۱-e^{-۲}}{۲} \approx ۰٫۴۳$ و $\frac{۱+e^{-۲}}{۲} \approx ۰٫۵۷$ برابرند. وانگهی، از آنچه بیان شد و نتیجهٔ ۱۰.۳ نیز چنین برمی‌آید که احتمال اینکه کلید رمز تعدادی زوج و ناصفر از حروف را ثابت نگه دارد، با همان حداکثر خطا، با مقدار تقریبی $\frac{۱}{۲}(۱ + e^{-۲}) - \frac{۱}{e} \approx ۰٫۲۰$ برابر است.

سپاسگزاری نویسندگان مقاله از داوران محترم، که پیشنهادها و نظرات ارزشمندشان برکیفیت مقاله افزود، کمال تشکر و قدردانی را دارند.

مراجع

[۱] آپوستل، تی. ام.، آنالیز ریاضی، ترجمهٔ علی‌اکبر عالم‌زاده، مؤسسهٔ انتشارات علمی دانشگاه صنعتی شریف، تهران، ۱۳۷۰.

[۲] استیوارت، ای.؛ تال، دی.، مبانی ریاضیات، ترجمهٔ محمدمهدی ابراهیمی، مرکز نشر دانشگاهی، تهران، ۱۳۶۵.

[۳] زیگلر، ال. ای.، تمرین‌هایی در نظریهٔ مجموعه‌ها، ترجمهٔ عظیم اهری و غلامحسین بهفروز، انتشارات نیما، تبریز، ۱۳۶۵.

[۴] سینکوب، آبراهام، آشنایی با رمزگشایی به روش ریاضی، ترجمهٔ رویا درودی و عبادالله محمودیان، مرکز نشر دانشگاهی، تهران، ۱۳۷۴.

[۵] لین، شوو ینگ‌تی.؛ لین، یو–فنگ، نظریهٔ مجموعه‌ها و کاربردهای آن، ترجمهٔ عمید رسولیان، مرکز نشر دانشگاهی، تهران، ۱۳۶۸.

[۶] نیون، ایی.، ریاضیات انتخاب، ترجمهٔ علی عمیدی و بتول جذبی، مرکز نشر دانشگاهی، تهران، ۱۳۶۸.

[۷] هالموس، پی. آر.، نظریهٔ طبیعی مجموعه‌ها، ترجمهٔ حمید دادالله، مرکز نشر دانشگاهی، تهران، ۱۳۶۲.

[۸] یوسف‌نیا، محمد، اثبات شرکت‌پذیری عمل تفاضل متقارن مجموعه‌ها، مجله رشد آموزش ریاضی، شمارهٔ ۴ (۱۳۶۵)، ۲۵–۲۶.

[9] Alsina, C., Trillas, E., On the symmetric difference of fuzzy sets, *Fuzzy Sets and Systems*, **153** (2005), 181-194.
[10] Bhat, B. R., *Modern Probability Theory: An Introductory Textbook*, Wiley Easten Limited, New Delhi, 1981.
[11] Feller, W., *An Introduction to Probability Theory and its Applications*, vol. 1, John Wiley and Sons, Inc., New York, 1968.
[12] Feller, W., *An Introduction to Probability Theory and its Applications*, vol. 2, John Wiley and Sons, Inc., New York, 1991.
[13] Folland, G. B., *Real Analysis: Modern Techniques and Their Applications*, 2nd ed., John Wiley and Sons, Inc., New York, 1999.
[14] Gaspar, M. B., Martin, F., A procedure for computing the symmetric difference of regions defined by polygonal curves, *J. Symbolic Comput.*, **61** (2014), 53-65.
[15] Givant, S., Halmos, P. R., *Introduction to Boolean Algebra*, Springer, New York, 2009.
[16] Hosseini, M., The associativity of the symmetric difference, *Math. Mag.*, **79** (2006), 391-392.
[17] Larson, H. J., *Introduction to Probability Theory and Statistical Inference*, 3rd ed., John Wiley and Sons, Inc., New York, 1982.
[18] Luciano, D., Gordon, P., Cryptography: from Caesar ciphers to public-key cryptosystems, *College Math. J.*, **18** (1987), 2-17.
[19] Williams, M., Difference sets and the symmetric difference, Master‘s thesis, Sam Houston State University, 2022.

علی پارسیان: دانشگاه تفرش، دانشکدهٔ ریاضی
رایانامه: parsian@tafreshu.ac.ir
زهرا پارسیان: دانشگاه شاهد، گروه مهندسی فناوری اطلاعات
رایانامه: zparsian313@gmail.com

Mathematical Culture and Thought
Volume 42, Number 72, Spring/Summer 2023, Pages 111–127
doi: 10.30504/mct.2022.1300.1907

Symmetric Difference, Cardinal, and Probability

A. Parsian[1]✉, Z. Parsian[2]

[1]Department of Mathematics, Tafresh University, Iran
[2]Department of Information Technology, Shahed University, Iran

Abstract. In the most mathematical texts, there have been paid less attention to "symmetric difference" and its properties. In this article, after verifying some basic properties of this operation, we provide a formula for computing the cardinal (res. probability) of the sets (res. events) obtained from the combination of symmetric difference of finite number of sets (res. events), in terms of the cardinal (res. probability) of the constituent sets (res. events). Finally, we end the article by an application in cryptography.

Keywords: cardinal, symmetric difference, probability, permutation, inclusion-exclusion principle, cryptography
Article history: Recieved 22 June 2022; Accepted 29 November 2022
Article type: original

References

[1] Alsina, C., Trillas, E., On the symmetric difference of fuzzy sets, *Fuzzy Sets and Systems*, **153** (2005), 181-194.

[2] Apostol, T. M., *Mathematical Analysis*, 5th printing, Addison-Wesley Publishing Company, Massachusetts, 1981.

[3] Bhat, B. R., *Modern Probability Theory: An Introductory Textbook*, Wiley Easten Limited, New Delhi, 1981.

[4] Feller, W., *An Introduction to Probability Theory and its Applications*, vol. 1, John Wiley and Sons, Inc., New York, 1968.

[1]parsian@tafreshu.ac.ir
[2]zparsian313@gmail.com

[5] Feller, W., *An Introduction to Probability Theory and its Applications*, vol. 2, John Wiley and Sons, Inc., New York, 1991.

[6] Folland, G. B., *Real Analysis: Modern Techniques and Their Applications*, 2nd ed., John Wiley and Sons, Inc., New York, 1999.

[7] Gaspar, M. B., Martin, F., A procedure for computing the symmetric difference of regions defined by polygonal curves, *J. Symbolic Comput.*, **61** (2014), 53-65.

[8] Givant, S., Halmos, P. R., *Introduction to Boolean Algebra*, Springer, New York, 2009.

[9] Halmos, P. R., *Naive Set Theory*, Springer, New York, 1998.

[10] Hosseini, M., The associativity of the symmetric difference, *Math. Mag.*, **79** (2006), 391-392.

[11] Larson, H. J., *Introduction to Probability Theory and Statistical Inference*, 3rd ed., John Wiley and Sons, Inc., New York, 1982.

[12] Lin, S. Y. T., Lin, Y., *Set Theory with Applications*, Mariner Publishing Company, Boston, 1981.

[13] Luciano, D., Gordon, P., Cryptography: from Caesar ciphers to public-key cryptosystems, *College Math. J.*, **18** (1987), 2-17.

[14] Niven, I., *Mathematics of Choice: Or, How to Count Without Counting*, Mathematical Association of America, Washington, DC, 1977.

[15] Sigler, L. E., *Exercises in Set Theory*, Springer-Verlag, New York, 1976.

[16] Sinkov, A., *Elementary Cryptanalysis: A Mathematical Approach*, Mathematical Association of America, Washington, DC, 1966.

[17] Stewart, I., Tall, D., *The Foundations in Mathematics*, 2nd ed., Oxford University Press, Oxford, 2015.

[18] Williams, M., Difference sets and the symmetric difference, Master‘s thesis, Sam Houston State University, 2022.

[19] Yūsifī, M., A proof for associativity of the symmetric difference, *Roshd Amūzish Rīyāzī*, **4** (1986), 25-26. [in Persian]