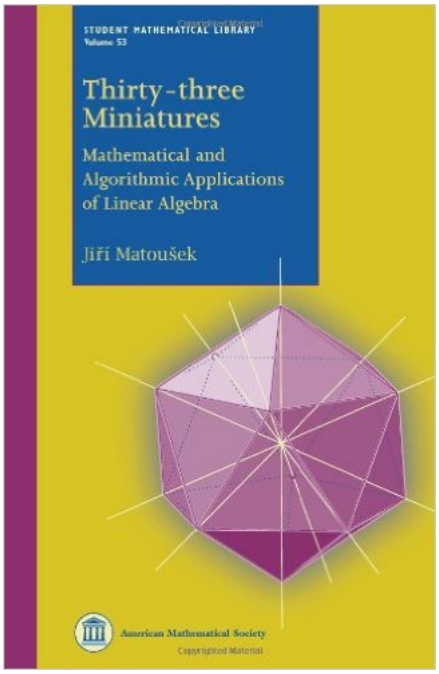
چهار نمونه از کاربردهای جبرخطی در دیگر شاخه‌های ریاضیات

عباس محرابیان

دانشگاه بریتیش کلمبیا

amehrabi@uwaterloo.ca

۲ آبان ۱۳۹۴



در این مقاله کتاب «سی‌وسه مینیاتور» را معرفی می‌کنیم. موضوع این کتاب ۱۸۰ صفحه‌ای کاربردهای جبرخطی در زمینه‌های دیگر مثل ترکیبیات، هندسه و طراحی الگوریتم است. کتاب از ۳۳ بخش کوتاه و مستقل تشکیل شده است و در هر بخش مسئله‌ای مطرح و حل کامل آن ارائه می‌شود. کتاب پر از ایده‌های جالب و هوشمندانه است و برخی راه‌حل‌ها واقعاً خارق‌العاده‌اند. خواننده پس از خواندن آن متقاعد می‌شود که داشتن نگاه جبرخطی‌ای می‌تواند خیلی کمک کند به حل مسائلی که ظاهراً بی‌ربط هستند. به خصوص چنین ایده‌هایی اخیراً در طراحی الگوریتم‌های سریع زیاد استفاده

می‌شود[۱] . جبرخطی استفاده شده در این کتاب، جبرخطی مقدماتی است.

نویسندهٔ کتاب Jiri Matousek از جمهوری چک است که متأسفانه چند ماه پیش درگذشت. او ۹ کتاب نوشته است و من سه تا از آن‌ها را دیده‌ام و همگی خیلی خوب نوشته شده‌اند. این کتاب هم مستثنی نیست. خواندن این کتاب برایم بسیار لذت‌بخش بود و در کنار کتاب روش احتمالاتی می‌توانم آن دو را جالب‌ترین کتاب‌های ریاضی که خواندم بنامم.[۲]

در این مقاله به عنوان مثال چهار تا از مسائلی که در کتاب طرح و حل شده‌اند را می‌آوریم. ابتدا چند تعریف که در طول مقاله استفاده خواهیم کرد را مرور می‌کنیم.

فرض کنید A یک ماتریس باشد. درایه‌ای[۳] از این ماتریس که در سطر iاُم و ستون jاُم قرار دارد را با $A_{i,j}$ نشان می‌دهیم. منظور از A^T، ترانهادهٔ[۴] این ماتریس است، و رتبهٔ[۵] این ماتریس را با $\mathrm{rank}(A)$ نشان می‌دهیم. ماتریس $n \times n$ همانی[۶] را با I_n نشان می‌دهیم. بردارها را به صورت ماتریس‌های ستونی تصور می‌کنیم. بنابراین اگر x, y دو بردار هم‌اندازه باشند، $x^T y$ همان ضرب داخلی x و y را نشان می‌دهد. مؤلفهٔ iاُم بردار x را با x_i نشان می‌دهیم.

۱ مثال اول: نظریهٔ مجموعه‌ها.

فرض کنید $A_1, \ldots, A_m$ زیرمجموعه‌هایی از مجموعهٔ $\{1, \ldots, n\}$ باشند که دو خاصیت دارند: تعداد اعضای هر یک از آن‌ها عددی فرد است، ولی هر دوتایی از آن‌ها تعداد زوجی عضو مشترک دارند. در این صورت اثبات کنید $m \leq n$.

این یک مسئلهٔ کاملاً ترکیبیاتی است که حل آن بدون استفاده از جبرخطی بسیار سخت است، در حالی که اثباتی بسیار کوتاه و هوشمندانه به کمک جبرخطی مقدماتی دارد که در زیر آمده است.

---

[۱] مثلاً ویدئوی روبرو را ببینید: https://simons.berkeley.edu/events/openlectures2014-fall-4

[۲] کتاب را به صورت رایگان دریافت کنید: http://kam.mff.cuni.cz/~matousek/stml-53-matousek-1.pdf

[۳] element

[۴] transpose

[۵] rank

[۶] identity

یک ماتریس $m \times n$ به نام M به صورت زیر تعریف می‌کنیم:

$$M_{i,j} = \begin{cases} ۱ & \text{if } j \in A_i \\ ۰ & \text{if } j \notin A_i. \end{cases}$$

به دلیل خواص مجموعه‌های $A_۱, \ldots, A_m$، می‌دانیم که هر سطری از M تعداد فردی ۱ دارد، و ضرب داخلی هر دو سطری از M تعداد زوجی ۱ دارد. بنابراین اگر M را به عنوان ماتریسی در میدان دو عضوی $\{۰, ۱\}$ در نظر بگیریم، آن‌گاه

$$M \times M^T = I_m$$

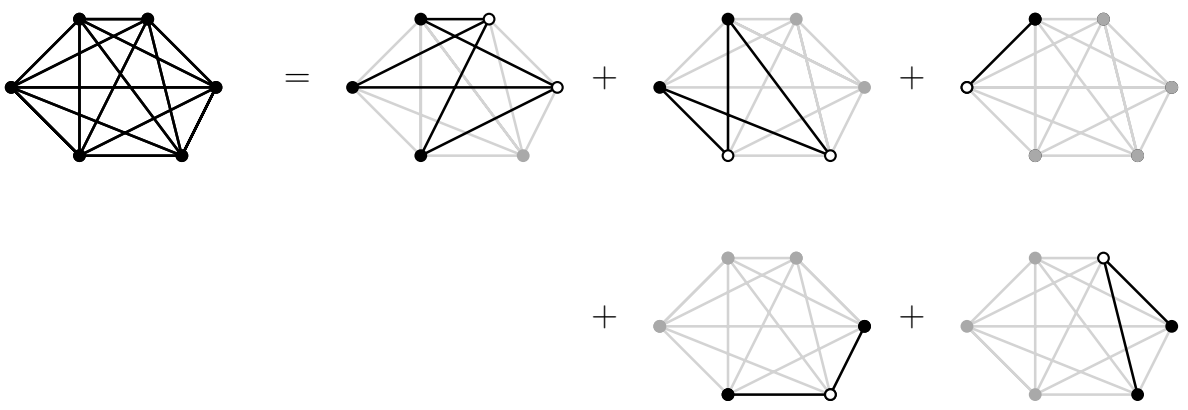
از این رابطه نتیجه می‌گیریم که رتبهٔ ماتریس M لااقل m است، چرا که توانسته‌ایم ماتریس I_m را به کمک ترکیب خطی ستون‌های آن تولید کنیم. (در حالت کلی برای هر دو ماتریس A و B که قابل ضرب کردن باشند، نامساوی زیر درست است: $\operatorname{rank}(A \times B) \leq \min\{\operatorname{rank}(A), \operatorname{rank}(B)\}$.)

از طرف دیگر، ماتریس M دارای n ستون است، بنابراین رتبهٔ آن نمی‌تواند بیشتر از n باشد. نتیجه می‌گیریم

$$m \leq \operatorname{rank}(M) \leq n.$$

۲ مثال دوم: نظریهٔ گراف.

یک گراف کامل[۷] گرافی است که همهٔ رئوس آن به هم وصلند، و یک گراف دوبخشی کامل[۸] گرافی است که رئوس آن را می‌توان به دو بخش ناتهی X و Y افراز کرد که همهٔ رئوس X به همهٔ رئوس Y وصلند و هیچ یال دیگری وجود ندارد. فرض کنید می‌خواهیم یال‌های یک گراف کامل را با زیرگراف‌های آن بپوشانیم، به طوری که زیرگراف‌ها همگی دوبخشی کامل باشند و هم‌چنین هر یال گراف اصلی در دقیقاً یکی از زیرگراف‌ها ظاهر شود. مثلاً در شکل زیر یک پوشش گراف کامل ۶ رأسی توسط ۵ زیرگراف آن را می‌توانید ببینید، و در حالت کلی می‌توان دید که یک گراف n رأسی کامل را می‌توان با $n - ۱$ زیرگراف دوبخشی کامل پوشاند. (اثبات به خواننده واگذار می‌شود!)



[۷] complete graph
[۸] complete bipartite graph

آیا پوششی با کم‌تر از $n-1$ زیرگراف وجود دارد؟ در این بخش با استفاده از جبرخطی نشان می‌دهیم که پاسخ منفی است. یک گراف n رأسی کامل با رئوس $\{1, 2, \ldots, n\}$ در نظر بگیرید و فرض کنید $H_1, H_2, \ldots, H_m$ زیرگراف‌های دوبخشی کاملی هستند که یال‌های آن را پوشانده‌اند. نشان می‌دهیم $m \geq n-1$.

برای هر k، فرض کنید X_k و Y_k دو بخش H_k باشند، بنابراین $X_k \cup Y_k = V(H_k) \subseteq \{1, \ldots, n\}$. برای هر k یک ماتریس $n \times n$ به نام $A^{(k)}$ به صورت زیر تعریف می‌کنیم

$$A^{(k)}_{i,j} = \begin{cases} 1 & \text{if } i \in X_k \text{ and } j \in Y_k \\ 0 & \text{otherwise.} \end{cases}$$

دقت کنید که چون H_k یک گراف دوبخشی کامل است، تمام سطرهای ناصفر $A^{(k)}$ با هم برابرند، در نتیجه رتبهٔ $A^{(k)}$ برابر ۱ است.

حال ماتریس $A = A^{(1)} + A^{(2)} + \cdots + A^{(m)}$ را در نظر بگیرید. هر سطر A را می‌توان به کمک ترکیب خطی سطرهای $A^{(1)}, A^{(2)}, \ldots, A^{(m)}$ تولید کرد، بنابراین رتبهٔ A حداکثر m است. برای تکمیل اثبات کافی است نشان دهیم رتبهٔ A دست‌کم $n-1$ است.

برای هر $1 \leq i < j \leq n$، یال بین رئوس i و j در دقیقاً یکی از H_kها ظاهر می‌شود، در نتیجه یکی از دو حالت زیر رخ می‌دهد: یا $A_{i,j} = 1$ و $A_{j,i} = 0$ و یا $A_{i,j} = 0$ و $A_{j,i} = 1$. همچنین داریم $A_{i,i} = 0$. نتیجه می‌گیریم $A + A^T = J_n - I_n$، که در آن J_n یک ماتریس $n \times n$ است که تمام درایه‌هایش ۱ است.

برای این که نشان دهیم رتبهٔ A دست‌کم $n-1$ است، از برهان خلف استفاده می‌کنیم. بدین منظور فرض کنید رتبهٔ A کم‌تر از $n-1$ است و فرض کنید B ماتریسی $(n+1) \times n$ باشد که n سطر اولش همان n سطر A هستند و همهٔ درایه‌های سطر آخرش ۱ هستند. چون B دقیقاً یک سطر جدید علاوه بر سطرهای A دارد، رتبهٔ آن حداکثر $n-1$ است. چون B دارای n ستون است، یک ترکیب خطی غیرصفر از ستون‌های B وجود دارد که برابر صفر می‌شود. به زبان ریاضی، بردار ناصفر $x \in \mathbb{R}^n$ وجود دارد که $Bx = 0$. در نتیجه $Ax = 0$ و به علاوه اگر مؤلفه‌های x را با $x_1, x_2, \ldots, x_n$ نشان دهیم، چون سطر آخر B تمامش ۱ است داریم $x_1 + x_2 + \cdots + x_n = 0$. از این تساوی نتیجه می‌گیریم $J_n x = 0$. پس از یک طرف داریم

$$x^T(A + A^T)x = x^T(J_n - I_n)x = x^T(J_n x) - x^T(I_n x) = 0 - x^T x = -\sum_{i=1}^{n} x_i^2 < 0,$$

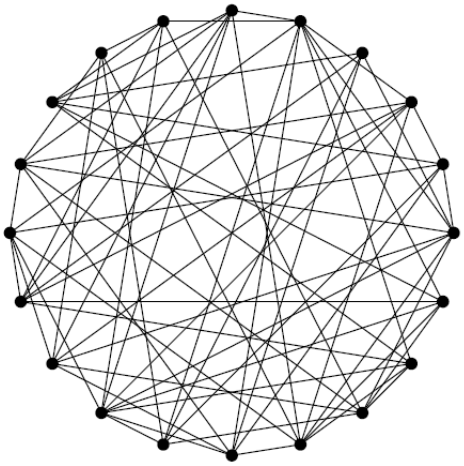
ولی از طرف دیگر می‌دانیم $Ax = 0$ پس

$$x^T(A + A^T)x = x^T(Ax) + (x^T A^T)x = x^T(Ax) + (Ax)^T x = 0.$$

این تناقض نشان می‌دهد رتبهٔ A دست‌کم $n-1$ است، و اثبات کامل می‌شود.

۳ مثال سوم: طراحی الگوریتم.

فرض کنید یک گراف داریم و می‌خواهیم ببینیم آیا مثلث دارد؟ یعنی آیا سه رأس وجود دارند که هر دو تایی به هم وصل باشند؟ توجه کنید که وقتی تعداد رئوس و یال‌ها زیاد باشد این مسئله اصلاً ساده نیست! مثلاً در گراف زیر آیا می‌توانید مثلث را پیدا کنید؟!



ساده‌ترین روشی که به ذهن می‌رسد اینست که برای هر سه‌تایی (x, y, z) از رئوس، بررسی کنیم که آیا هر سه یال xy, xz, yz در گراف هستند یا نه. این الگوریتمی از مرتبهٔ $n^۳$ است (تعداد سه‌تایی‌ها برابر است با $\binom{n}{۳}$ که برای nهای بزرگ بسیار به $n^۳/۶$ نزدیک است). آیا الگوریتمی وجود دارد که خیلی سریع‌تر باشد؟ در ادامه می‌بینیم که پاسخ مثبت است، و جالب است بدانید تمام الگوریتم‌هایی که تابحال ارائه شده‌اند و مرتبه‌شان از $n^۳$ کم‌تر است، جبری هستند و از الگوریتم‌های ضرب سریع ماتریس‌ها استفاده می‌کنند!

فرض کنید رئوس گراف را از ۱ تا n شماره‌گذاری کرده‌ایم، و وصل بودن رئوس را با نماد $\sim$ نشان می‌دهیم. ماتریس مجاورت[۹] گراف را با A نشان می‌دهیم و به صورت زیر تعریف می‌کنیم:

$$A_{i,j} = \begin{cases} ۱ & \text{if } i \sim j \\ ۰ & \text{if } i \not\sim j. \end{cases}$$

همچنین برای هر رأس i تعریف می‌کنیم $A_{i,i} = ۰$. دقت کنید که A یک ماتریس $n \times n$ است و به صورت یکتا گراف را مشخص می‌کند. تعریف کنید $B = A^۲$. طبق تعریف،

$$B_{i,j} = \sum_{k=۱}^{n} A_{i,k} A_{k,j} \qquad (۱)$$

که برابر با صفر است اگر و تنها اگر هیچ رأسی مثل k وجود نداشته باشد که $A_{i,k} = A_{k,j} = ۱$. در حقیقت، $B_{i,j}$ دقیقاً برابر است با تعداد همسایه‌های مشترک رئوس i و j. بنابراین اگر ماتریس B را داشته باشیم، برای فهمیدن این که آیا

[۹] adjacency matrix

گرافمان مثلث دارد یا نه، کافی است تمام زوج‌رأس‌ها را بررسی کنیم: اگر زوج (i,j) از رئوس وجود داشتند که $A_{i,j} > ۰$ و $B_{i,j} > ۰$ آن‌گاه می‌فهمیم که مثلثی با رئوس i و j (و یک رأس دیگر که پیدا کردنش ساده است) وجود دارد، وگرنه گرافمان مثلث ندارد. واضح است که بررسی کردن تمام زوج‌رأس‌ها نیاز به زمانی از مرتبهٔ $n^۲$ دارد، پس اگر بتوانیم به سرعت ماتریس B را محاسبه کنیم، می‌توانیم به سرعت وجود مثلث یا نبود آن را در گراف دریابیم. پس پرسشی که باید پاسخ دهیم اینست: برای محاسبهٔ ماتریس B به چقدر زمان نیاز داریم؟

دقت کنید که اگر بخواهیم از طریق تعریف ضرب ماتریس‌ها، یعنی فرمول (۱) ماتریس B را محاسبه کنیم، برای محاسبهٔ هر درایه به زمانی از مرتبهٔ n نیاز داریم، بنابراین محاسبهٔ کل B به زمانی از مرتبهٔ $n^۳$ نیاز دارد! ولی الگوریتم‌های هوشمندانه‌ای طراحی شده‌اند که ضرب دو ماتریس مربعی دلخواه را در زمان کوتاه‌تری محاسبه می‌کنند. اولین بار در سال ۱۹۶۹ استراسن[۱۰] الگوریتمی برای ضرب ماتریس‌ها ارائه کرد که زمان اجرایش از مرتبهٔ $n^{۲/۸۰۷}$ است. این الگوریتم بر ایده‌ای ساده ولی بسیار هوشمندانه استوار است؛ اگر آن را ندیده‌اید، به ویکی‌پدیا رجوع کنید.[۱۱] در سال‌های اخیر روی مسئلهٔ ضرب ماتریس‌ها بسیار کار شده است چرا که این عمل پایهٔ بسیاری از الگوریتم‌های جبری است و اگر زمان اجرای آن بهتر شود زمان اجرای الگوریتم‌های بسیاری بهتر می‌شوند. بهترین الگوریتمی که در حال حاضر وجود دارد از مرتبهٔ $n^{۲/۳۷۳}$ است.[۱۲] بنابراین با استفاده از این الگوریتم می‌توان الگوریتمی از همین مرتبه برای مسئلهٔ پیدا کردن مثلث در گراف طراحی کرد، که به مراتب از الگوریتم بدیهی «بررسی تمام سه‌تایی‌ها از رئوس» سریع‌تر است.

فرض کنید ω کوچک‌ترین عددی باشد به طوری که الگوریتمی از مرتبهٔ n^ω برای ضرب دو ماتریس $n \times n$ وجود دارد. در حال حاضر مقدار دقیق ω مشخص نیست ولی می‌دانیم $۲ \leq \omega < ۲/۳۷۳$. الگوریتم بالا سریع‌ترین الگوریتم شناخته شده برای یافتن مثلث در گراف‌های چگال[۱۳] است، یعنی گراف‌هایی که تعداد یال‌هایشان به مراتب از تعداد رئوسشان بیشتر است. برای گراف‌هایی که این طوری نیستند (مثلاً گراف‌های مسطح، که نسبت تعداد یال‌ها به رئوسشان از عدد ثابتی کم‌تر است) الگوریتم‌های سریع‌تری وجود دارند: برای هر گرافی که m یال دارد، الگوریتمی از مرتبهٔ $m^{۲\omega/(\omega+۱)}$ برای یافتن مثلث وجود دارد.

مسئلهٔ یافتن یک گراف خاص به عنوان زیرگرافی از یک گراف ورودی را می‌توان برای گراف‌های دیگری به غیر از مثلث هم مطرح کرد، و تحقیقات گسترده‌ای در نظریهٔ الگوریتم‌ها در این باره انجام شده است. مثلاً جالب است بدانید که الگوریتمی از مرتبهٔ $n^۲$ وجود دارد که یا یک دور چهار رأسی را در گراف ورودی پیدا می‌کند یا به درستی تشخیص می‌دهد که گراف هیچ دوری به طول چهار ندارد.

۴ مثال چهارم: هندسه.

فرض کنید R مستطیلی با اضلاع ۱ و x باشد به طوری که x عددی گنگ است. در این صورت آیا می‌توان R را با تعداد متناهی مربع فرش کرد؟ یعنی آیا می‌توان تعدادی مربع درون R گذاشت به طوری

---

[۱۰] Volker Strassen

[۱۱] https://en.wikipedia.org/wiki/Strassen_algorithm

[۱۲] برای بیشتر دانستن دربارهٔ تاریخچهٔ این مسئله و بهترین الگوریتم موجود برای حل آن، می‌توانید به این صفحهٔ ویکی‌پدیا رجوع کنید:
https://en.wikipedia.org/wiki/Coppersmith-Winograd_algorithm

[۱۳] dense

که مربع‌ها تمام R را بپوشانند و فقط در مرز اشتراک داشته باشند؟ در این بخش به کمک جبرخطی نشان می‌دهیم که پاسخ منفی است.

اثبات از طریق برهان خلف است. فرض کنید $Q_1, Q_2, \ldots, Q_n$ تعدادی مربع باشند که R را فرش می‌کنند، و فرض کنید s_i طول اضلاع Q_i باشد.

مجموعهٔ اعداد حقیقی $\mathbb{R}$ را می‌توان به عنوان یک فضای برداری روی میدان اعداد گویا $\mathbb{Q}$ در نظر گرفت. جمع و ضرب در این فضا همان جمع و ضرب معمولی هستند. این فضای برداری بی‌نهایت‌بُعدی است و شاید کمی نامتعارف باشد ولی برای حل این مسئله کارگشاست! دقت کنید که اعداد گویای p و q وجود ندارند که $p \times 1 + q \times x = 0$، بنابراین 1 و x در این فضا مستقل خطی هستند.

فرض کنید $V \subseteq \mathbb{R}$ زیرفضای تولید شده توسط $\{x, s_1, \ldots, s_n\}$ باشد. به عبارت دیگر،

$$V = \{q_1 s_1 + \cdots + q_n s_n + q_{n+1} x : q_1, q_2, \ldots, q_{n+1} \in \mathbb{Q}\} .$$

چون 1 و x مستقل خطی هستند، می‌توان یک نگاشت خطی مثل $f : V \to \mathbb{R}$ در نظر گرفت که $f(1) = 1$ و $f(x) = -1$. مثلاً، فرض کنید $\{b_1, \ldots, b_k\}$ یک پایه[14] برای V باشد و $b_1 = 1$ و $b_2 = x$. در این صورت می‌توان تعریف کرد

$$f(b_1) = 1, f(b_2) = -1, f(b_3) = \ldots, f(b_k) = 0 ,$$

و سپس f را به صورت خطی روی Vگسترش داد.

برای هر مستطیل A با اضلاع $a, b \in V$ تعریف می‌کنیم

$$v(A) = f(a)f(b) .$$

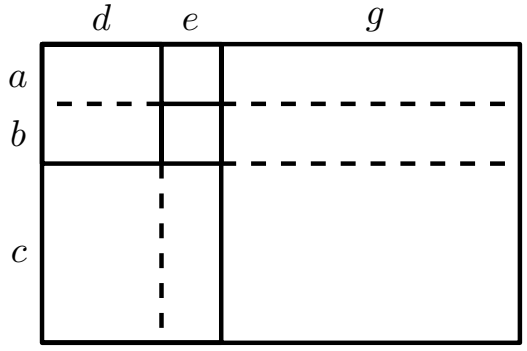
ادعا می‌کنیم داریم

$$v(R) = \sum_{i=1}^{n} v(Q_i) \qquad (2)$$

اگر این معادله درست باشد به تناقض می‌رسیم زیرا $v(R) = f(1)f(x) = -1$ در حالی که برای هر i بین 1 و n داریم $v(Q_i) = v(s_i)^2 \geq 0$.

[14] basis

برای اثبات (۲)، همهٔ اضلاع مربع‌بندی فرضی را تا مرز R گسترش می‌دهیم، بدین صورت:



با این کار R به تعدادی مستطیل افراز می‌شود، و با توجه به خطی بودن f، می‌توان دید که $v(R)$ برابر است با حاصل جمع مقدار v روی همهٔ مستطیل‌های کوچک. مثلاً در شکل بالا،

$$\begin{aligned} v(R) &= f(a+b+c)f(d+e+g) \\ &= f(a)f(d) + f(a)f(e) + f(a)f(g) + f(b)f(d) \\ &+ f(b)f(e) + f(b)f(g) + f(c)f(d) + f(c)f(e) + f(c)f(g)\,. \end{aligned}$$

به همین ترتیب، برای هر مربع Q_i، مقدار $v(Q_i)$ برابر است با حاصل جمع مقدار v روی همهٔ مستطیل‌های کوچک داخل Q_i. مثلاً در شکل بالا، پنج مربع داریم و مقدار v آن‌ها به ترتیب از راست به چپ و از بالا به پایین برابر است با:

$$\begin{aligned} f(g)f(a+b+c) &= f(g)f(a) + f(g)f(b) + f(g)f(c), \\ & f(e)f(a), \\ & f(e)f(b), \\ f(e+d)f(c) &= f(c)f(e) + f(c)f(d), \\ f(d)f(a+b) &= f(a)f(d) + f(b)f(d), \end{aligned}$$

در نتیجه (۲) ثابت می‌شود.