دانشکده علوم ریاضی
دانشگاه صنعتی شریف

تحقیق در عملیات ۱

محمدهادی فروغمنداعرابی
پاییز ۱۳۹۹

برنامه‌ریزی خطی در کدها

جلسه هفدهم

نگارنده: سپهر محمدخانی

۱ مروری بر مباحث گذشته

در سه جلسه‌ی پیشین کاربردهایی از برنامه‌ریزی خطی در نظریه‌ی بازی‌ها، اثبات قضایایی در نظریه‌ی گراف و الگوریتمی تقریبی برای زمان‌بندی بیان شد. در ادامه به کاربردی از برنامه‌ریزی خطی در کدگذاری می‌پردازیم.

۲ انگیزه

در مخابره یا ذخیره‌سازی داده، ممکن است داده‌ای که به دست گیرنده رسیده است یا از حافظه خوانده شده، دقیقاً همان داده‌ی اولیه نباشد و با مقداری خطا روبرو باشیم. هدف، ممکن ساختن بازیابی داده‌ی اولیه با وجود خطا است.

مثال ۱. *فرض کنید می‌خواهیم ۴ بیت را مخابره کنیم. اگر هر بیت را سه بار تکرار کنیم، در صورت رخ دادن خطا در انتقال ۱ بیت، داده‌ی اولیه قابل بازیابی است.*
داده‌ی دریافت شده با حداکثر یک بیت خطا: 111001000111
پس در بیت قرمز شده خطا رخ داده و داده‌ی اولیه قابل بازیابی است: 111001000111

مسئله در حالت کلی، انتقال یکی از N حالت ممکن با n بیت است که اگر در حداکثر r بیت خطا رخ داد، حالت مورد نظر قابل بازیابی باشد.

۳ کدگذاری

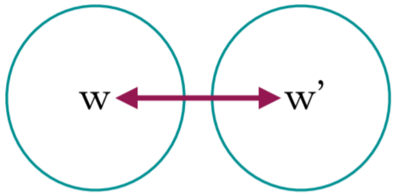
تعریف ۲. *برای دو رشته‌ی $w, w' \in \{0,1\}^n$ به ترتیب فاصله‌ی همینگ [1] و وزن به صورت زیر تعریف می‌شود:*

$$d_H(w,w') = |\{j \in \{1,...,n\} : w_j \neq w'_j\}|$$
$$|w| = |\{j \in \{1,...,n\} : w_j = 1\}|$$

از تعریف نتیجه می‌شود $d_H(w,w') = |w \oplus w'|$ که $w \oplus w' = ((w_1+w'_1)\ mod\ 2, ..., (w_n+w'_n)\ mod\ 2)$.

تعریف ۳. *به هر $C \subset \{0,1\}^n$ یک کد می‌گوییم و می‌گوییم C فاصله‌ی d را دارد اگر برای هر دو رشته‌ی متمایز w, w' در C، $d_H(w,w') \geq d$. $A(n,d)$ بیشینه کاردینال کدی مانند $C \subset \{0,1\}^n$ با فاصله‌ی d تعریف می‌شود.*

فرض کنید کدی با فاصله‌ی d داریم. آنگاه خطای کمتر از $\frac{d}{2}$ را می‌توانیم تصحیح کنیم.



مثال ۴. *فاصله‌ی همینگ بین هر دو رشته‌ی متمایز حداقل ۱ است؛ پس $A(n,1) = 2^n$.*
حداقل فاصله‌ی بین دو رشته به طول n و با تعداد فردی بیت ۱، ۲ است. از طرفی، در هر زیرمجموعه از $\{0,1\}^n$ با کاردینال بیشتر از 2^{n-1}، حداقل دو رشته با فاصله‌ی ۱ وجود دارد (طبق لانه کبوتری)؛ پس $A(n,2) = 2^{n-1}$.

می‌دانیم $5312 \leq A(17,3) \leq 6552$، در ادامه تلاش می‌کنیم که اثبات کنیم ۶۵۵۲ یک کران بالا برای $A(17,3)$ است.

۴ کران بالا برای A(n,d)

لم ۵ (Sphere-packing bound)**.** *برای هر n, r*

$$A(n, 2r+1) \leq \lfloor \frac{2^n}{\Sigma_{i=0}^{r}\binom{n}{i}} \rfloor$$

اثبات. فرض کنید $C \subset \{0,1\}^n$ کدی با فاصله‌ی $2r+1$ باشد. برای هر رشته‌ی $w \in C$، در فاصله‌ی i از w، $\binom{n}{i}$ رشته وجود دارد. طبق تعریف C، برای هر دو رشته‌ی $w, w' \in C$، هیچ رشته‌ای در $\{0,1\}^n$ وجود ندارد که فاصله‌اش از هر دو رشته‌ی w, w' کمتر یا مساوی r باشد. پس حداقل به تعداد $|C|\Sigma_{i=0}^{r}\binom{n}{i}$ عضو در $\{0,1\}^n$ وجود دارد و در نتیجه $|C| \leq \lfloor \frac{2^n}{\Sigma_{i=0}^{r}\binom{n}{i}} \rfloor$. □

کران بالای به دست آمده برای $A(17,3)$ از لم بالا برابر است با ۷۲۸۱. در ادامه با استفاده از برنامه‌ریزی خطی به کرانی بهتر دست می‌یابیم.

قضیه ۶ (The Delsarte bound)**.** *برای هر اعداد صحیح n, i, t که $0 \leq i, t \leq n$، قرار دهید*

$$K_t(n,i) = \sum_{j=0}^{min(i,t)} (-1)^j \binom{i}{j}\binom{n-i}{t-j}.$$

آنگاه برای هر n, d، مقدار بهینه‌ی برنامه‌ی ذیل با متغیرهای $x_0, ..., x_n$، یک کران بالای $A(n,d)$ است:

[1] Hamming distance

$$\begin{array}{ll} Maximize & x_0 + x_1 + ... + x_n \\ subject\ to & x_0 = 1 \\ & x_i = 0, \qquad\qquad i = 1, 2, ..., d-1 \\ & \Sigma_{i=0}^{n} K_t(n, i) \,.\, x_i \geq 0, \qquad t = 1, 2, ..., n \\ & x_0, x_1, ... x_n \geq 0 \end{array}$$

یک کد C با فاصله‌ی d در نظر بگیرید. برای اثبات قضیه کافی است تعبیری مناسب از متغیرهای برنامه‌ی بالا برای کد C ارائه کنیم؛ یعنی x_iها را طوری از روی C تعریف کنیم که در قیود برنامه صدق کنند و $|C| \leq x_0 + ... + x_n$.
با توجه به این که برای $0 < i < d$، $x_i = 0$، و این که برای هر $w \in C$ هیچ کلمه‌ای در C با فاصله‌ی $0 < i < d$ از w وجود ندارد، تعریف x_iها به صورت زیر مناسب به نظر می‌آید:

$$x_i = |\{(w, w') \in C^2 : d_H(w, w') = i\}|$$

اما طبق این تعریف

$$\begin{array}{ll} x_0 = |\{(w, w) \in C^2\}| = |C| & \\ x_i = 0, & i = 1, 2, ..., d-1 \\ x_0 + x_1 + ... + x_n = \Sigma_{i=0}^{n} |\{(w, w') \in C^2 : d_H(w, w') = i\}| = |\{(w, w') \in C^2\}| = |C|^2 & \end{array}$$

پس اگر تعریف را به صورت زیر بازنویسی کنیم:

$$x_i = \frac{1}{|C|} |\{(w, w') \in C^2 : d_H(w, w') = i\}|$$

داریم

$$\begin{array}{ll} x_0 = 1 & \\ x_i = 0, & i = 1, 2, ..., d-1 \\ x_0 + x_1 + ... + x_n = |C| & \end{array}$$

نشان می‌دهیم این تعریف دیگر قیود را نیز برآورده می‌کند.

لم ۷. *فرض کنید $I \subset \{1, ..., n\}$ مجموعه‌ای از اندیس‌ها است و $C \subset \{0, 1\}^n$. آنگاه تعداد $(w, w') \in C$ که $d_H^I(w, w')$ عددی فرد است، کمتر یا مساوی تعداد $(w, w') \in C$ است که $d_H^I(w, w')$ زوج است (منظور از $d_H^I(w, w')$ تعداد اندیس‌های $i \in I$ است که $w_i \neq w'_i$)*

اثبات. تعریف کنید $|w|_I = |\{i \in I : w_i = 1\}|$ و $E = \{w \in C : |w|_I\ is\ even\}$ و $O = \{w \in C : |w|_I\ is\ odd\}$.
طبق رابطه‌ی $d_H^I(w, w') = |w \oplus w'|_I$، $d_H^I(w, w')$ زوج است اگر و تنها اگر $|w|_I$ و $|w'|_I$ زوجیت یکسانی داشته باشند (هر دو عضو E یا هر دو عضو O باشند)؛ پس تعداد $(w, w') \in C$ که $d_H^I(w, w')$ عددی زوج است برابر با $|E|^2 + |O|^2$ است و تعداد $(w, w') \in C$ که $d_H^I(w, w')$ عددی فرد است برابر با $2|E||O|$. از طرفی، $|E|^2 + |O|^2 - 2|E||O| = (|O| - |E|)^2 \geq 0$. □

نتیجه ۸. *برای هر $C \subset \{0, 1\}^n$ و هر $v \in \{0, 1\}^n$ داریم*

$$\sum_{(w, w') \in C^2} (-1)^{(w \oplus w')^T v} \geq 0$$

اثبات. کافی است قرار دهید $I = \{i : v_i = 1\}$، در این صورت $(w \oplus w')^T v = d_H^I(w, w')$ و مجموع مورد نظر برابر است با تعداد $(w, w') \in C$ که $d_H(w, w')$ زوج است، منهای تعداد آن‌هایی که $d_H(w, w')$ فرد است. پس حکم از لم قبل نتیجه می‌شود.
اثباتی دیگر: توجه کنید که زوجیت $(w \oplus w')^T v$ با زوجیت $(w + w')^T v$ یکسان است. پس

$$\sum_{(w, w') \in C^2} (-1)^{(w \oplus w')^T v} = \sum_{(w, w') \in C^2} (-1)^{(w + w')^T v} =$$
$$= \sum_{(w, w') \in C^2} (-1)^{w^T v} \,.\, (-1)^{w'^T v} = (\sum_{w \in C} (-1)^{w^T v})^2 \geq 0.$$

□

اثبات قضیه ۶. طبق نتیجه‌ی قبل

$$\circ \le \sum_{v\in\{\circ,1\}^n:|v|=t} \; \sum_{(w,w')\in C^2} (-1)^{(w\oplus w')^T v} = \sum_{(w,w')\in C^2} \; \sum_{v\in\{\circ,1\}^n:|v|=t} (-1)^{(w\oplus w')^T v}$$

برای یک $u = w \oplus w'$ ثابت، تعریف کنید $i = |u| = d_H(w,w')$ و یک عدد j در نظر بگیرید. بردار v که $u^T v = j$ و $|v| = t$ ، به این صورت است که در j اندیس مانند k که $u_k = 1$ برابر ۱ و بقیه‌ی $t-j$ مولفه‌ی برابر ۱ آن در بین $n-i$ مولفه‌ی برابر ۰ بردار u قرارد دارد؛ پس تعداد بردارهایی مانند v برابر است با

$$\binom{i}{j}\binom{n-i}{t-j}$$

و در نتیجه برای (w,w') که $d_H(w,w') = i$

$$\sum_{v\in\{\circ,1\}^n:|v|=t} (-1)^{(w\oplus w')^T v} = \sum_{j=\circ}^{min(i,t)} (-1)^j \binom{i}{j}\binom{n-i}{t-j} = K_t(n,i)$$

پس

$$\circ \le \sum_{(w,w')\in C^2} K_t(n,i)$$

توجه کنید تعداد دفعاتی که $K_t(n,i)$ در جمع بالا ظاهر می‌شود برابر است با تعداد زوج کلماتی که از هم فاصله‌ی i دارند که طبق تعریف متغیرهای x_i برای کد C ، برابر است با $x_i|C|$؛ پس اگر $|C|$ را از دو طرف ساده کنیم به همان قید مورد نظر می‌رسیم

$$\circ \le \sum_{i=\circ}^{n} K_t(n,i) \; . \; x_i$$

□

کران بالای به دست آمده از قضیه‌ی بالا برای $A(17,3)$ برابر است با $6553\frac{3}{5}$ و می‌دانیم $A(17,3)$ باید عددی صحیح باشد؛ پس $A(17,3) \le 6553$. حال سعی می‌کنیم این کران را یک عدد، کمتر کنیم!
فرض خلف کنید که کد $C \subset \{\circ,1\}^{17}$ با فاصله‌ی ۳ وجود دارد که $|C| = 6553$. توجه کنید که جمع تعداد فردی از اعداد ۱− و ۱ نمی‌تواند برابر ۰ شود و تعداد اعضای C فرد است؛ پس

$$(\sum_{w\in C} (-1)^{w^T v})^2 \ge 1$$

که بهبود یافته‌ی نامساوی انتهای نتیجه۸ است. اگر در اثبات قضیه‌ی پیشین از این نامساوی بهبود یافته به جای نامساوی نتیجه۸ استفاده کنیم، نتیجه می‌شود

$$\sum_{i=\circ}^{n} K_t(n,i) \; . \; x_i \ge \frac{\binom{n}{t}}{|C|}$$

پس اگر در برنامه‌ریزی خطی ارائه شده، قیود $\sum_{i=\circ}^{n} K_t(n,i) \; . \; x_i \ge \circ$ را با $\sum_{i=\circ}^{n} K_t(n,i) \; . \; x_i \ge \frac{\binom{n}{t}}{6553}$ جایگزین کنیم، این برنامه یک جواب شدنی دارد (x_iهای به دست آمده از کد C). اما جواب بهینه‌ی این برنامه $6552\frac{3}{5}$ است که با فرض $|C| = 6553$ در تناقض است؛ پس $A(17,3) \le 6552$.
۶۵۵۲ بهترین کران شناخته شده برای $A(17,3)$ است.

۵ مراجع و منابع

[1] Jiří Matoušek and Bernd Gärtner. Understanding and Using Linear Programming. Springer-Verlag Berlin Heidelberg, 1st edition, 2007.

[۲] اسلایدهای جلسه‌ی هفدهم