بسم الله الرحمن الرحيم

دانشکده ریاضی و کامپیوتر
بخش ریاضی

پایان‌نامه تحصیلی برای دریافت درجه کارشناسی ارشد
رشته ریاضی محض گرایش جبر

کدگذاری، فضاهای شیفت و گراف‌ها

نگارش
نوشین دربان مقامی

استاد راهنما
دکتر نصرت الله شجره‌پور صلواتی

آذر ماه ۱۳۹۱

این پایان نامه به عنوان یکی از شرایط درجه کارشناسی ارشد به

بخش ریاضی

دانشکده ریاضی و کامپیوتر
دانشگاه شهید باهنر کرمان

تسلیم شده و هیچگونه مدرکی به عنوان فراغت از تحصیل دوره مزبور شناخته نمی شود.

دانشجو: نوشین دربان مقامی امضاء:

استاد راهنما: دکتر نصرت الله شجره‌پور صلواتی امضاء:

داور اول : نداریم امضاء:

داور دوم: نداریم امضاء:

نماینده تحصیلات تکمیلی: نداریم امضاء:

تقدیم به

- پدر بزرگوار و مادر مهربانم

آن دو فرشته ای که از خواسته هایشان گذشتند، سختی ها را به جان خریدند و خود را سپر بلای مشکلات و ناملایمات کردند تا من به جایگاهی که اکنون در آن ایستاده ام برسم

- همسرم، اسطوره زندگیم، پناه خستگیم و امید بودنم
- و دختر عزیزم

تشکر و قدردانی

سپاس و ستایش سزاوار پروردگار مهربان است که هستی را در پاکی مطلق خویش و بر پایه‌ی دانش وعدالت آفرید و به بشر آموخت که نیل به خوشبختی درگرو اندیشیدن وپیمودن راه است. او را در برابر بی نهایت یاری ها وگره گشایی های مهربانانه اش سپاس بی کران می گویم.

سپاس بی پایان بر استاد ارجمندم جناب آقای دکتر نصرت‌الله شجره‌پور صلواتی که دراین مدت از محضر علمی واخلاقی ایشان بهره بردم و همواره خود را مدیون زحمات ایشان می دانم و به خاطر راهنمایی واهتمام ارزشمندشان در مسیر رشد علمی ام، سپاسگزارم.

همچنین از زحمات اساتید محترم کمال تشکر و سپاسگزاری را دارم.

نوشین دربان مقامی

nooshinmaghami@yahoo.com

مقدمه

مفهوم فضای شیفت، اولین بار در کارهای هادامارد [1] و مورس [2] برای مدل سازی شارهای ژئودزیکی مورد مطالعه قرار گرفت. امروزه فضاهای شیفت از اهمیت خاصی در مبحث سیستم های دینامیکی برخوردار است اما ما در اینجا از این مفهوم برای معرفی روشی در ذخیره و انتقال داده ها استفاده خواهیم کرد.

در عصر جدید، سیستمهای ارتباطی و اطلاعاتی بر پایه انتقال ارزان، سریع و مطمئن داده ها بنا شده اند. یکی از مهمترین مفاهیم مرتبط با این سیستمها که با اهداف یاد شده در ارتباط است، مفهوم کدگذاری است. به زبان ساده، کدگذاری یک ضابطه برای تغییر یک پیام به پیام جدید می باشد که معمولاً پیام جدید در یک الفبای جدید و یا در الفبای پیام اولیه تعریف می شود. امروزه روش های زیادی در کدگذاری معرفی شده اند که از آن جمله می توان به کدگذاری خطی و کدگذاری جبری اشاره کرد. اصولاً تمام این روش ها دارای یک ماهیت بوده و فقط روش های آنالیز این مفاهیم متفاوت است.

در اینجا سعی می کنیم کدهای مختلف روی فضاهای شیفت را معرفی کرده و شرایط وجود و یا هم ارزی این کدها را بررسی کنیم. در ادامه رابطه ای بین فضاهای شیفت و گراف ها ایجاد خواهیم کرد و در پایان بعضی از مفاهیم تعریف شده در فضاهای شیفت را که روی گروه ها پیاده شده اند، معرفی می کنیم.

---

[1] Hadamard

[2] Morse

چکیده

در این پایان‌نامه به بررسی روشهای کدگذاری با استفاده از فضاهای شیفت می‌پردازیم. همچنین رابطه‌ای دوطرفه بین گراف‌ها و فضاهای شیفت ایجاد می‌کنیم و در پایان نیز تعمیم این مفاهیم روی گروهها را ارائه می‌دهیم.

کلمات کلیدی: *فضای شیفت، کد بلوکی اسلایدی، آنتروپی، گراف، رنگ‌آمیزی گروه*

فهرست مطالب

۱ مقدمات و پیش نیازها **۱**

۱.۱ نظریه گروهها ۱

۲.۱ کدگذاری ۶

۳.۱ ذخیره داده‌ها ۱۳

۲ فضاهای شیفت و گراف‌ها **۱۸**

۱.۲ تعاریف ۱۸

۲.۲ شیفت بلوکی بالاتر ۲۵

۳.۲ کد بلوکی لغزان ۲۶

۴.۲ کدگذارهای پیچشی ۳۴

۵.۲ شیفتهای از نوع متناهی ۳۹

۶.۲ گراف ها و شیفتهای آنها ۴۴

۷.۲ نمایش گرافی شیفتهای از نوع متناهی ۵۲

۸.۲ آنتروپی ۵۶

۳ کدهای متناهی به یک **۶۰**

۱.۳ شیفتهای سافیک ۶۰

۲.۳ کدهای بلوکی لغزان متناهی به یک ۶۲

۴ فضاهای شیفت روی گروهها **۷۰**

۱.۴ تبدیلات شیفت ۷۰

۲.۴ فضاهای شیفت ۷۱

۳.۴ آنتروپی ۷۳

واژه‌نامه انگلیسی به فارسی **۷۴**

واژه‌نامه فارسی به انگلیسی **۷۶**

فهرست تصاویر

۱.۱ قسمتی از گراف کیلی $\mathbb{Z}$ ۳

۲.۱ قسمتی از گراف کیلی $\mathbb{Z} \times \mathbb{Z}$ ۳

۳.۱ قسمتی از گراف کیلی روی دو مولد، هر تقاطع نشانگر یک عنصر گروه است. . ۵

۴.۱ معادل عددی حروف ابجد ۹

۵.۱ دیسک گردان ۱۴

۶.۱ ذخیره‌سازی و بازیابی داده ها ۱۵

۷.۱ مقایسه کدگذارهای FM و MFM ۱۶

۱.۲ گرافی که یک فضای شیفت را تعریف می کند. ۲۱

۲.۲ کد بلوکی لغزان ۲۷

۳.۲ ایده اثبات ۴۲

۴.۲ گراف معمولیG ۴۵

۵.۲ گراف یک r-شیفت کامل ۴۸

۶.۲ گراف متناظر با ماتریس A ۴۸

۷.۲ یک گراف تحویل پذیر ۵۱

۸.۲ گراف شیفت میانگین طلایی مجدداً کدگذاری شده ۵۳

۹.۲ گرافهای یالی بالاتر شکل ۶.۲ . . . . . ۵۴

۱.۳ یک الماس گرافی ۶۵
۲.۳ یک الماس ۶۶
۳.۳ گرافهای به طور منحصربفرد قابل کدگشایی ۶۹

فصل ۱

مقدمات و پیش نیازها

۱.۱ نظریه گروهها

گروه $\mathcal{G} = (G, .)$ یک مجموعه از عناصر G و یک عملگر دوتایی . روی G با خواص زیر است:

۱- برای هر $a, b, c \in G$ ، $a.(b.c) = (a.b).c$.

۲- برای هر $a \in G$ ، $e \in G$ موجود است به طوریکه $e.a = a.e = a$.

۳- برای هر $a \in G$ ، $a^{-1} \in G$ موجود است به طوریکه $a.a^{-1} = a^{-1}.a = e$.

معمولاً نماد "." را حذف می کنیم و به جای $a.b$ می نویسیم ab بعلاوه تا زمانی که هیچ ابهامی در مورد عملگر دوتایی نباشد، مجموعه G را یک گروه می نامیم.

تعریف ۱.۱.۱. دو گروه $(G_1, .)$ و $(G_2, *)$ یکریخت هستند اگر یک نگاشت دوسویی $\phi : G_1 \to G_2$ موجود باشد به طوریکه برای هر $x, y \in G$ ، $\phi(x.y) = \phi(x) * \phi(y)$ تابع ϕ یک یکریختی نامیده می شود .

برای اهداف ما، گروههای $(G_1, .)$ و $(G_2, *)$ یکسان در نظر گرفته می شوند اگر یکریخت باشند.

در گروه $\mathcal{G} = (G, .)$ عملگر '.' می تواند به صورتهای مختلفی تعریف شود. برای گروههای متناهی '.' می تواند به صورت نوشتار صریح یک جدول ضرب تعریف شود، اما این برای گروههای نامتناهی صادق نیست ولی می توانیم '.' را با یک نمایش تعریف کنیم. یک روش دیگر برای معرفی یک گروه، یک نمایش از گروه به صورت $< \sigma | R >$ است که در آن σ مجموعه مولدها است به‌طوری‌که هر عنصر گروه را می‌توان به صورت حاصلضرت توان‌هایی از مولدها نوشت و R مجموعه روابط بین این مولدهاست.

مثال ۲.۱.۱. گروه اعداد صحیح تحت جمع، $\mathbb{Z}$ ، می تواند به صورت $< \sigma | \emptyset >$ نمایش داده شود که در آن $\sigma = \sigma_1$. همچنین این نمایش را می توان به صورت $< \sigma_1 | >$ نوشت. حتی اگر عملگر دوتایی برای این گروه جمع باشد، می توان به جای $\sigma_1 + \sigma_1$ ، عناصر را به صورت $\sigma_1 \sigma_1 = \sigma_1^2$ نوشت. بنابراین هر عنصر با ضابطه σ_1^n برای یک $n \in \mathbb{Z}$ است.

مثال ۳.۱.۱. گروه دوری از مرتبه n ، C_n ، می تواند به صورت $< \sigma_1 | \sigma_1^n = e >$ نشان داده شود.

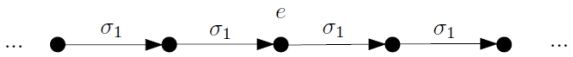
مثال ۴.۱.۱. گروه دیریکله D_n ، که تقارنهای یک n -ضلعی منتظم را نشان می دهد، می تواند به صورت زیر نمایش داده شود:

$$< r, s | r^2 = e, s^n = e, (rs)^n = e >$$

هر گروه همچنین می تواند با یک گراف کیلی نمایش داده شود. یک گراف کیلی $C = (V, E)$ از یک گروه G عبارت است از یک مجموعه V از رأسها و یک مجموعه E از یالها بطوریکه هر رأس یک عنصر منحصر بفرد از G را نمایش می دهد.
دو رأس $g_1, g_2 \in G$ با یک یال برچسب خورده σ_i از g_1 به g_2 ، به هم وصل می شوند اگر و تنها اگر $g_1 \sigma_i = g_2$.
بنابراین هر رأس دقیقاً دارای یک یال ورودی و خروجی برای هر σ_i است. توجه کنید که

این یالها به نمایش G بستگی خواهند داشت.

مثال ۱.۱.۵. شکل ۱.۱ ، بخشی از گراف کیلی برای $\mathbb{Z}$ با نمایش $< \sigma_1 | >$ را نشان می دهد که در آن اعضای گروه با دایره های سیاه رنگ مشخص شده اند.

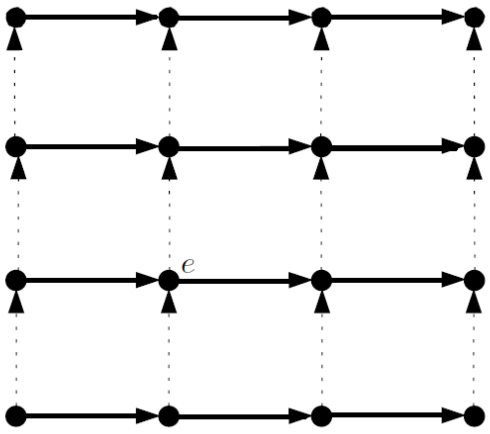


شکل ۱.۱ : قسمتی از گراف کیلی $\mathbb{Z}$

مثال ۱.۱.۶. شکل ۲.۱ بخشی از گراف کیلی را برای $\mathbb{Z} \times \mathbb{Z}$ با نمایش

$$< \sigma_1, \sigma_2 | \sigma_1\sigma_2 = \sigma_2\sigma_1 >$$

نشان می دهد. در شکل ۲.۱ ، عناصر گروه (رأسها) با دایره های سیاه نشان داده شده اند. فرض می کنیم فلشهای سیاه با برچسب σ_1 و فلشهای نقطه چین با برچسب σ_2 باشند.



شکل ۲.۱ : قسمتی از گراف کیلی $\mathbb{Z} \times \mathbb{Z}$

زمانی که یک نمایش برای هر گروه موجود باشد، بسیاری مانند $R - \{0\}$ تحت ضرب، نیازمند کاردینال متناهی σ یا R هستند. چنین گروههایی آنالیز بسیار مشکلی دارند. بنابراین ما در اینجا توجهمان را محدود به گروههای با تولید متناهی می کنیم.

تعریف ۷.۱.۱. گروه G با تولید متناهی است اگر یک نمایش $< \sigma|R >$ از G موجود باشد به طوریکه $|\sigma|$ و $|R|$ متناهی باشند.

در گروههای با تولید متناهی می توانیم اندازه یک عنصر گروه، $|g|$ را تعریف کنیم:

$$|g| = min\{n : g = \sigma_{a_1}\sigma_{a_2}...\sigma_{a_n}\}$$

با استقرا می گوییم: $|e| = 0$.

به طور شهودی، $|g|$ متناظر است با تعداد یالهایی که باید روی گراف کیلی G پیمود تا از e به g رسید.

به هر حال مقدار $|g|$ ممکن است به نمایش G بستگی داشته باشد.

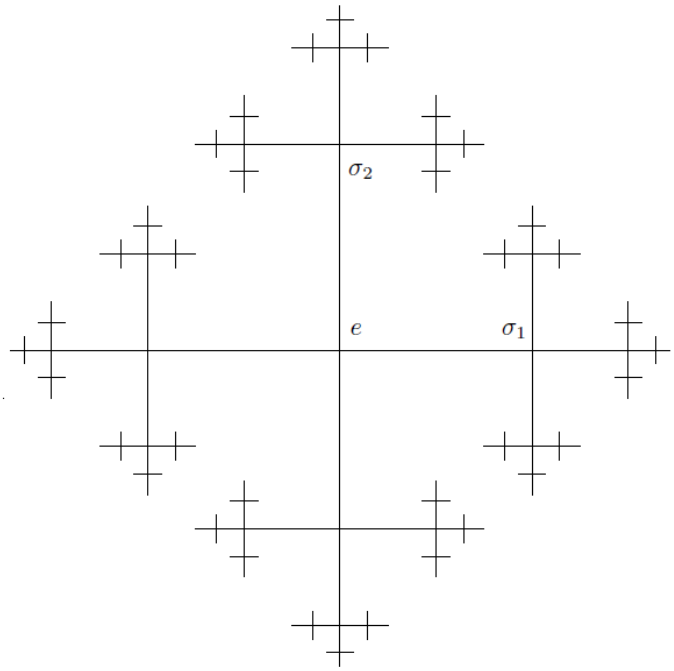
تعریف ۸.۱.۱. یک گروه آزاد، گروه دلخواه G است که می تواند به صورت $< \sigma|\emptyset >=<$ $< \sigma| >$ نمایش داده شود. اگر $|\sigma| = q$ باشد، می گوییم G یک گروه آزاد از مرتبه q است.

در هر گروه آزاد، مجموعه R از روابط تهی است بنابراین هر حاصلضرب $\sigma_{a_1}\sigma_{a_2}...\sigma_{a_n}$ یک عنصر منحصر به فرد از گروه را می دهد.

قسمتی از گراف کیلی روی دو مولد در شکل ۳.۱ نشان داده شده است.

تعریف ۹.۱.۱. یک گروه $\mathcal{H} = (H, .)$ یک زیر گروه از گروه $\mathcal{G} = (G, .)$ است اگر $H \subset G$ و $e \in H$ و اگر $x, y \in H$ ، آنگاه $xy \in H$ و $x^{-1} \in H$.

مثال ۱۰.۱.۱. $\mathbb{Z}$ در حد یکریختی، یک زیر گروه $\mathbb{Z} \times \mathbb{Z}$ است. این به وضوح دیده می شود زیرا در $< \sigma_1, \sigma_2|\sigma_1\sigma_2 = \sigma_2\sigma_1 >$ می توانیم عناصر را به شکل σ_1^n در نظر بگیریم، که به سادگی، گروه $\mathbb{Z}$ است.



شکل ۱.۳: قسمتی از گراف کیلی روی دو مولد، هر تقاطع نشانگر یک عنصر گروه است.

مثال ۱.۱.۱۱. فرض کنیم $\mathcal{G} = C_{۱۲}$ گروه دوری از مرتبه ۱۲ باشد. آنگاه $C_۴, C_۳, C_۲$ و $C_۶$ زیر گروههای $\mathcal{G}$ هستند.

تعریف ۱.۱.۱۲. اندیس یک زیر گروه $H \subset G$ ، کاردینال مجموعه $\{aH | a \in G\}$ است. اگر اندیس H متناهی باشد، H زیرگروه با اندیس متناهی نامیده می شود.

بنابراین در یک گروه متناهی، اندیس زیر گروه بدیهی ، کاردینال گروه است.
در گروههای نامتناهی، اندیس زیر گروه شامل e ، نامتناهی است. برای هر گروه G ، G یک زیر گروه با اندیس متناهی از اندیس ۱ است. در اینجا یک مثال بدیهی ارائه می دهیم.

مثال ۱.۱.۱۳. فرض کنید G با $< \sigma_۱, \sigma_۲ | \sigma_۱\sigma_۲ = \sigma_۲\sigma_۱, \sigma_۲^k = e >$ برای یک ثابت k نمایش داده شود. در G ، $< \sigma_۱ | >$ یک زیرگروه با اندیس متناهی از اندیس k است و $< \sigma_۲ | \sigma_۲^k = e >$ یک زیرگروه از اندیس نامتناهی است.

فرض کنیم H یک زیر گروه از G باشد. هر مجموعه (aH) که در آن $a \in G$ ، یک

همرده از H نامیده می شود. گروه همرده های چپ H که با G/H نشان داده می شود، شامل همه عناصر به شکل (aH) است که در آن $a \in G$. عملگر دوتایی '.' تعریف شده روی G/H به صورت $(aH).(bH) = (abH)$ تعریف می شود.

به طور مشابه، گروه همرده های راست H به صورت $G\backslash H$ نمایش داده می شود و شامل همه عناصر به شکل (Ha) است که در آن $a \in G$. عملگر '.' روی $G\backslash H$ به صورت $(Ha).(Hb) = (Hab)$ تعریف می شود.

۲.۱ کدگذاری

اولین نکته ای که در رابطه با پیامها باید به آن توجه داشت، ایجاد یک مدل ریاضی ساده برای یک پیام می باشد. ما این کار را در فصل های آینده با استفاده از فضاهای شیفت انجام خواهیم داد.

مثال ۱.۲.۱. بسیاری از پیامها به زبانهای طبیعی نظیر فارسی، انگلیسی یا فرانسوی نوشته می شوند. این پیامها شامل نمادهایی بوده که کلمات را ساخته و کلمات نیز جملاتی مانند همین جمله را به وجود می آورند. ارسال یک پیام از فردی به فرد دیگر از راه های مختلفی امکان پذیر می باشد؛ به عنوان مثال به صورت یک یادداشت دست نویس یا یک نامه الکترونیک. یک پیام متنی نیز به همین شکل بوده ولی اغلب با یک زبان غیر طبیعی بیان می شود.

مثال ۲.۲.۱. دستگاههایی مانند اسکنرها و دوربینهای دیجیتال، پیامهایی را در غالب نمادهای الکترونیک تولید می کنند. این پیامها از طریق سیمها یا فیبرهای نوری یا به وسیله امواج رادیویی از یک دستگاه به دستگاه دیگر ارسال می شوند.

ما یک پیام را به صورت دنباله ای از نمادها می پنداریم که در آن هیچ چیز، به جز ترتیب این نمادها، اهمیت ندارد.

وظیفه یک پیام انتقال اطلاعات از یک فرستنده به یک گیرنده است. به منظور انجام موفق این وظیفه، فرستنده و گیرنده بایستی بر روی یک مجموعه واحد از نمادها به توافق برسند. این مجموعه، الفبا نامیده می شود.

مثال ۳.۲.۱. ما مجموعه الفبای فارسی، شامل ۳۳ نماد (حروف ا، ب، پ،...،ی و یک فضای خالی که آن را با □ نمایش می دهیم) را مجموعه A می نامیم. اغلب به دلیل سادگی از مجموعه A برای نمایش یک پیام به زبان فارسی استفاده می کنیم ولی واضح است که برخی ویژگیهای زبان نادیده گرفته شده اند. به این ترتیب از تفاوت قایل شدن بین حروف بزرگ و کوچک و علائم نگارشی نیز صرف نظر می کنیم. البته برای نمایش یک پیام فارسی در غالب رشته ای از نمادهای الفبا، برخی اصلاحات نیز انجام می گیرد. به عنوان مثال، جمله

کلمه امیدواری اغلب به درستی به کار نمی رود

با استفاده از نمادهای الفبا (مجموعه A) ، به صورت زیر آورده می شود:
ک ل م ه □ ا م ی د و ا ر ی □ ا غ ل ب □ ب ه □ د ر س ت ی □ ب ه □ ک ا ر □ ن م ی ر و د □

مثال ۴.۲.۱. مجموعه الفبای B دارای دو نماد ۰ و ۱ بوده $(B = \{۰, ۱\})$ که رقم دودویی یا بیت نامیده می شوند. چون این بیتها به صورت الکترونیک با وضعیتهای روشن و خاموش قابل پیاده سازی هستند، به عنوان الفبای اصلی تمامی برنامه های کاربردی جدید به کار می روند. در عمل، بیتها در قالب گروه های بزرگتری مانند کلمات ۳۲ بیتی با هم ترکیب می گردند. اما هر پیامی که به صورت الکترونیک منتقل می گردد، خواه به صورت یک نامه الکترونیک از یک دوست یا یک تصویر ماهواره ای که به زمین ارسال می شود، الزاماً دنباله ای از بیتها است.

به صورت ساده می توان گفت که کدگذاری، قانونی برای جایگزینی یک پیام با پیام

دیگر می باشد. پیام دوم می تواند از همان الفبای پیام اول استفاده کرده یا الفبای جدیدی را برای خود تعریف کند.

مثال ۵.۲.۱. یک مثال ساده برای کدگذاری پیام در الفبای ۳۳ نمادی A ، می تواند در قالب استفاده از همان الفبا و با برعکس نوشتن هر کلمه (از آخر به اول) تعریف شود. به عنوان مثال پیام

ا ی ن □ ی ک □ پ ی ا م □ ن م و ن ه □ ا س ت

به صورت زیر در می آید :

ن ی ا □ ک ی □ م ا ی پ □ ه ن و م ن □ ت س ا

مثال ۶.۲.۱. یک قانون برای کدگذاری پیامهای الفبای A با استفاده از الفبای B می تواند به این ترتیب باشد که: حروف دارای نقطه را با صفر و حروف بدون نقطه را با یک، جایگزین کرده و از فاصله صرف نظر می کنیم. بر اساس این قانون، جمله

ا ی ن □ ی ک □ پ ی ا م □ ن م و ن ه □ ا س ت

به جمله زیر تبدیل می شود:

۰۱۱۱۰۱۱۰۱۱۱۰۱۱۰۱۱

مثال ۷.۲.۱. یکی از قدیمی ترین روشهای کدگذاری حروف الفبا در زبانهای فارسی و عربی، استفاده از حروف ابجد است. ابجد شیوه ای برای مرتب سازی حروف زبان فارسی و عربی است که در آن، حروف بر پایه الفبای اولیه خط فنیقی مرتب شده اند. گاهی از این

حرف	معادل عددی	حرف	معادل عددی	حرف	معادل عددی	حرف	معادل عددی
ا	١	ح	٨	س	٦٠	ت	٤٠٠
ب	٢	ط	٩	ع	٧٠	ث	٥٠٠
ج	٣	ی	١٠	ف	٨٠	خ	٦٠٠
د	٤	ک	٢٠	ص	٩٠	ذ	٧٠٠
ه	٥	ل	٣٠	ق	١٠٠	ض	٨٠٠
و	٦	م	٤٠	ر	٢٠٠	ظ	٩٠٠
ز	٧	ن	٥٠	ش	٣٠٠	غ	١٠٠٠

شکل ۴.۱: معادل عددی حروف ابجد

شیوه در شماره گذاری موارد یا صفحات به کار می رود. در این روش، معادل با هر حرف الفبا، عددی بین ۱ تا ۱۰۰۰ در نظر گرفته شده و برای کدگذاری یک کلمه، از حاصل جمع اعداد مربوط به هر حرف استفاده می گردد. به عنوان مثال، برای کدگذاری کلمه « رایانه » در این روش، ابتدا معادل عددی هر حرف از جدول ۴.۱ به دست آمده:

$$ر = ۲۰۰،ا = ۱،ی = ۱۰،ا = ۱،ن = ۵۰،ه = ۵$$

سپس با جمع کردن این اعداد، کد مربوط به کلمه مورد نظر به دست می آید:

$$۲۰۰ + ۱ + ۱۰ + ۱ + ۵۰ + ۵ = ۲۶۷$$

اکنون می توانیم برخی مفاهیم اصلی را به درستی تعریف نماییم:

تعریف ۸.۲.۱. الفبا مجموعه ای متناهی مانند S بوده که عناصر آن نمادها می باشند.

تعریف ۹.۲.۱. یک پیام یا کلمه یا رشته در الفبای S ، دنباله ای متناهی از عناصر آن