بسم الله الرحمن الرحیم

دانشکده علوم ریاضی
گروه ریاضی کاربردی

پایان‌نامه کارشناسی ارشد

گرایش کدگذاری

عنوان

شمارش دورهای کوتاه در پروتوگراف‌های کدهای شبه دوری خلوت

پژوهشگر

مسعود جلیل

استاد راهنما

دکتر محمد غلامی

استاد مشاور

دکتر مهدی کدیور

آذر ۱۳۹۲

به پاس عاطفه سرشار و گرمای امید بخش وجودشان، که در این سردترین روزگاران بهترین پشتیبان است،
به پاس قلب های بزرگشان، که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می گراید،
و به پاس ایثار و محبت های بی دریغشان، که هرگز فروکش نمی کند،
این مجموعه را به پدر و مادرم تقدیم می کنم.

اولین چکه ناودان بلند یک احساس را، در قالب کلامی از جنس تنفس با غنچه های معصوم یاس، به روی حجم سپید یک برگه می ریزم و آن را به لحظه های همه ی پروانه صفتهای این گیتی بی انتها به آستان نیلوفری دلهای زلال هدیه می کنم:

ای یزدان پاک تو را سپاس می گویم،

که به حکمت بی انتهایت مرا یاری کردی،

و به رحمت نعمتهایت را بر من تمام کردی،

خانواده ای خوب به من عطا کردی که در هر حال پشتیبانی ام کنند و استادانی سر راهم نهادی تا دانش و علمشان را بی ریا در اختیارم بگذارند.

بر خود لازم می دانم از همه عزیزانی که در جهت به سرانجام رساندن این رساله مرا یاری نمودند، قدردانی نمایم. مراتب قدردانی و سپاس خود را از زحمات بی دریغ استاد راهنمای بزرگوارم جناب آقای دکتر محمد غلامی ابراز می نمایم. از استاد گرانقدر، جناب آقای مهدی کدیور که زحمت مطالعه و مشاوره این مجموعه را تقبل فرمودند کمال امتنان را دارم، همچنین از استادان گرانقدر، دکتر آهنجیده و دکتر رئیسی که زحمت داوری این رساله را بر عهده داشتند، قدردانی می نمایم.

با آرزوی موفقیت برای تمام عزیزان

معود جلیل

آذر ۱۳۹۲

چکیده

در این پایانامه روشی کارا برای شمارش تعداد دورهای کوتاه در گراف بدوی کدهای شبه دوری خلوت ارائه می‌دهیم؛ این روش که مبتنی بر رابطه‌ی بین تعداد دورهای کوتاه در گراف و مقادیر ویژه‌ی ماتریس وقوع است، را بیان می‌کنیم. در این روش به منظور کاهش پیچیدگی محاسبه‌ی مقادیر ویژه ماتریس وقوع از ویژگی‌های ماتریس دوری بلوکی استفاده می‌کنیم. نتایج بدست آمده نشان می‌دهند پیچیدگی محاسبات در این روش نسبت به روش‌های موجود تا حدود زیادی کاهش می‌یابد. همچنین نشان می‌دهیم که میانگین توزیع دور در گراف تنر کدهای شبه دوری خلوت نسبت به کدهای تصادفی بیشتر است.

رده بندی موضوعی ریاضی ۲۰۱۰: 46H05، 46H40، 46K05، 46J05.

کلمات کلیدی : گراف بدوی، کدهای شبه دوری خلوت،کمرگراف

فهرست مطالب

مقدمه

موضوع کدهای خلوت[1] اولین بار توسط گالاگر[2] در سال ۱۹۶۲ مطرح شد [۲]، ولی برای مدت بیشتر از ۳۰ سال تقریبا به فراموشی سپرده شد. در واقع پیچیدگی کاربری این کدها در آن زمان، آن‌ها را از توانایی رقابت با سایر کدها بازداشته بود و باعث شده بود که این دسته از کدها در کاربردهای عملی مورد توجه قرار نگیرند [۱۳، ۱، ۸].
تنر[3] در سال ۱۹۸۱ با گسترش این کدها و معرفی آن‌ها با یک نمایش گرافی به نام گراف تنر عملا به روشی موثر در کاربردهای عملی به منظور کدگذاری و کدگشایی این کدها دست یافت [۱، ۳]. عمدتا وجود دورهای با طول کم در این نمایش گرافی در الگوریتم کدگشایی مطلوب نبوده و پیچیدگی محاسباتی و احتمال شکست الگوریتم را افزایش می‌دهد [۳، ۱۷، ۵، ۶]. بنابراین در کدهای خلوت، کمرگراف[4] در گراف تنر کد، به جهت به کارگیری تعداد تکرارهای کمتر در الگوریتم کدگشایی برای رسیدن به جواب، یکی از پارامترهای مهم طراحی این کدهاست [۵، ۴]. از دیگر موارد مهم در طراحی کدهای خلوت، داشتن کمترین فاصله[5] بالاست؛ زیرا این پارامتر باعث تصحیح خطای بیشتر در انتقال اطلاعات می‌شود
در سال ۱۹۹۵، مک کی[6] و نیل[7] دوباره کدهای خلوت را مورد توجه قرار داده و نشان دادند که این کدها علاوه بر داشتن یک ساختار ساده می‌توانند رقیبی جدی برای کدهای توربو[8]در میل به حد شانون باشند [۲۳]. در سال‌های اخیر پژوهش‌های بسیاری در رابطه با گراف های بدوی صورت گرفته است. از جمله ساخت گراف بدوی متناظر با کد خلوت، رابطه ی بین ماتریس بررسی توازن کد و دورهای موجود در گراف بدوی، و نیز شمارش کوتاه‌ترین دورها در گراف بدوی کدهای خلوت می‌توان اشاره کرد. یکی از مهم‌ترین نتایج به دست آمده در این باره این است که هر چه اندازه‌ی کوتاه‌ترین دور در گراف تنر یک کد کمتر باشد، کدگشایی کد مربوطه آسان‌تر خواهد بود. بر این اساس، موضوع شمارش و یافتن دور در گراف بدوی مورد توجه است.
در سال‌های اخیر، روش های ساختاری و الگوریتم های بسیاری در این زمینه مطرح شده‌اند. برای مثال هالفورد[9] در سال ۲۰۰۵ مقاله‌ای ارائه داد که تعداد دورهای موجود در گراف‌های دوبخشی را محاسبه

1. LDPC Code
2. Galager
3. Tanner
4. Girth
5. Minimum Distance
6. MacKay
7. Neal
8. Turbo Code
9. Halford

می‌کند. بنی هاشمی و کریمی نیز الگوریتم‌هایی را در این خصوص معرفی کردند [۱۳، ۱۲].
درفصل اول این پایان‌نامه ابتدا تعاریف و مفاهیم اولیه که در فصل‌های آتی مورد نیاز است را بیان می‌کنیم [۱۱، ۲۱، ۲۲]. در فصل دوم چگونگی ساخت کدهای خلوت را بر اساس گراف بدوی مورد بحث و بررسی قرار می‌دهیم [۱۶، ۳]. در فصل سوم ساختار کدهای خلوت شبه دوری[1] را بر مبنای ماتریس‌های جایگشتی چرخشی[2] مورد بحث و بررسی قرار می‌دهیم [۵، ۱]. و سپس قضایای فسریر[3] را برای کوتاه‌ترین دورهای به طول حداقل ۶، ۸، ۱۰ و ۱۲ مورد بحث و بررسی قرار می‌دهیم. در نهایت در فصل چهارم روشی برای به دست آوردن کوتاه‌ترین دور در گراف اولیه متناظر با آن ارایه می‌دهیم و سپس با مثال‌هایی نتایج به دست آمده از این روش را مورد بررسی قرار می‌دهیم [۱۲، ۱۹].

1. Quasi Cyclic LDPC Code
2. Circulant Permutation Matrices
3. Fossorier

فهرست نمادها

فصل ۱

مفاهیم اولیه

اهداف کلی فصل

در این فصل ابتدا به بیان مفاهیم گروه، میدان، فضای برداری، گراف و قضایایی می‌پردازیم که در فصول آتی پایان‌نامه از آن‌ها استفاده خواهیم‌کرد و سپس با معرفی کدهای بلوکی خطی، کدهای دوری و شبه دوری؛ ماتریس مولد و ماتریس بررسی توازن این کدها را به‌دست می‌آوریم. در ادامه کدهای خلوت، که رده‌ی مهمی از کدهای بلوکی خطی هستند را با ارائه نمایش ماتریسی و گرافی از این کدها، معرفی می‌کنیم [۲، ۲۴، ۲۵].

۱.۱ گروه، میدان و فضای برداری

تعریف ۱.۱.۱. هر تابع $f: G \times G \longrightarrow G$ را یک عمل دوتایی روی مجموعه‌ی غیرتهی G می‌نامند.

تعریف ۲.۱.۱. یک **گروه** $(G, *)$ متشکل از یک مجموعه‌ی غیرتهی و یک عمل دوتایی $*$ است که روی مجموعه‌ی G تعریف شده و شرایط زیر برقرار است:

۱) برای هر $a, b \in G$ داشته باشیم

$$a * b \in G.$$

۲) برای هر $a, b, c \in G$ خاصیت شرکت پذیری داریم

$$a * (b * c) = (a * b) * c.$$

۳) برای هر $a \in G$ عضوی چون e در G وجود داشته باشد به‌طوری که برای

$$e * a = a * e = a.$$

۴) برای هر $a \in G$ عضوی چون $a^{-۱}$ در G وجود داشته باشد به‌طوری که

$$a * a^{-۱} = a^{-۱} * a = e.$$

در تعریف بالا عناصر e و $a^{-۱}$ را به‌ترتیب عضو همانی و عضو وارون، نسبت به عمل $*$ در G می‌نامند.

تعریف ۳.۱.۱. گروه $(G, *)$ را یک گروه آبلی یا تعویض پذیر می‌نامند، هرگاه برای هر $a, b \in G$ داشته باشیم:

$$a * b = b * a.$$

تعریف ۴.۱.۱. تعداد اعضای یک گروه متناهی G، مرتبه‌ی گروه G نامیده می‌شود و با $| G |$ نمایش داده می‌شود.

تعریف ۵.۱.۱. اگر F مجموعه ای از عناصر باشد که دو عمل جمع "+" و ضرب "." روی آن تعریف شده باشد، آن‌گاه مجموعه F با عمل دوتایی + و . میدان[1] نامیده می‌شود اگر شرایط زیر برقرار باشند:

۱. F تحت عمل + یگ گروه جابجایی باشد. عنصر همانی تحت عمل + عنصر صفر میدان F نامیده می‌شود و با ۰ نمایش داده می‌شود.

۲. مجموعه $F/\{۰\}$ تحت عمل ضرب یک گروه جابجایی باشد. عنصر همانی نسبت به عمل ضرب عنصر یکه میدان F نامیده می‌شود و با ۱ نمایش داده می‌شود.

۳. برای هر سه عضو b, c و a از میدان F شرط زیر برقرار باشد.

$$a.(b + c) = a.b + a.c \tag{۱.۱}$$

خاصیت (۳) را قانون توزیع یا توزیع ضرب روی جمع نامیده می‌شود .

1. Field

تعریف ۶.۱.۱. مجموعه‌ی غیرتهی V را روی میدان F یک **فضای برداری** می‌نامند، هرگاه شرایط زیر برقرار باشند:

۱) V یک گروه آبلی تحت عمل جمع باشد،

۲) برای هر عضو a از F و هر عضو v در V، $a.v$ یک عضو در V باشد،

۳) برای هر عضو a و b در F و هر عضو v در V، قانون شرکت پذیری زیر برقرار باشد،
$$(a.b).v = a.(b.v).$$

۴) برای هر عضو a در F و عضوهای v و u در V، توزیع زیر برقرار باشد،
$$a.(u+v) = a.u + b.v.$$

۵) برای هر دو عضو a و b در F و عضو v در V، توزیع زیر برقرار باشد،
$$(a+b).v = a.v + b.v.$$

۶) با فرض این‌که ۱ عضو واحد (همانی) F باشد، برای هر عضو v در V، رابطه‌ی $1.v = v$ برقرار باشد.

عناصر V، بردار و عناصر میدان F، اسکالر نامیده می‌شوند، هم‌چنین عمل جمع روی V را جمع برداری و عمل ضرب بین یک اسکالر از F و یک بردار از V را ضرب اسکالر می‌نامند.

تعریف ۷.۱.۱. فرض کنید S یک زیرمجموعه غیرتهی از فضای برداری V روی میدان F باشد، در این‌صورت S را زیرفضایی از V می‌نامند، هرگاه S، خود تحت اعمال جمع و ضرب اسکالر تعریف شده بر V، یک فضای برداری باشد.

قضیه ۸.۱.۱. *اگر برای هر دو بردار u و v در S، $u+v$ نیز برداری در S باشد و هم‌چنین برای هر اسکالر a در F و بردار v در S، $a.v$ نیز متعلق به S باشد، آن‌گاه S یک زیرفضای برداری نامیده می‌شود.*

برهان. به مرجع [۲۴] بخش ۳۰۴ قضیه ۱ مراجعه شود. □

تعریف ۹.۱.۱. اگر v_1، v_2، …، v_k بردارهایی از فضای برداری V و a_1، a_2، …، a_k، k اسکالر دلخواه در میدان F باشند، آن‌گاه a_1v_1، a_2v_2، …، a_kv_k و مجموع $a_1v_1 + a_2v_2 + \ldots + a_kv_k$، بردارهایی در V هستند. به‌علاوه جمع بالا، ترکیب خطی بردارهای v_1، v_2، …، v_k نامیده می‌شود.

تعریف ۱۰.۱.۱. مجموعه بردارهای v_1، v_2، …، v_k از فضای برداری V روی میدان F مستقل خطی نامیده می‌شوند اگر و تنها اگر برای هر k اسکالر a_i، $1 \leq i \leq k$ در F، $a_1v_1 + a_2v_2 + \ldots + a_kv_k = 0,$ نتیجه دهد؛ $a_1 = a_2 = \ldots = a_k = 0$ در غیر این‌صورت این بردارها را وابسته خطی می‌نامیم.

تعریف ۱۱.۱.۱. یک مجموعه از بردارها، فضای برداری V روی میدان F را تولید می‌کند، هرگاه بتوان هر بردار از فضای برداری V را به‌صورت ترکیب خطی از بردارهای این مجموعه نوشت.

تعریف ۱.۱.۱۲. در هر فضای برداری حداقل یک مجموعه از بردارهای مستقل خطی وجود دارد که فضا را تولید می‌کند، چنین مجموعه‌ای را یک پایه برای فضای برداری می‌نامند.
لازم به ذکر است که دو پایه متمایز از یک فضای برداری، دارای تعداد مساوی بردار مستقل خطی هستند.

تعریف ۱.۱.۱۳. تعداد بردارهای مستقل خطی یک پایه از فضای برداری را بعد فضای برداری می‌نامند، در این‌صورت اگر یک پایه از فضای برداری V دارای n بردار مستقل خطی باشد، و آن را با $\dim V = n$.

نمایش می‌دهیم.

تعریف ۱.۱.۱۴. فرض کنید A یک ماتریس از مرتبه $m \times n$ باشد، در این‌صورت:

۱) رتبه سطری (ستونی) ماتریس A برابر بیشترین تعداد سطرهای (ستون‌های) مستقل خطی در ماتریس A است؛ هم‌چنین رتبه سطری و ستونی A با هم برابر هستند که به‌طور ساده آن‌را رتبه ماتریس نامیده و با $\text{rank}(A)$ نمایش داده می‌شود، بنابراین:
$$۱ \leq \text{Rank}(A) \leq \min(m, n),$$

۲) ماتریس A را با رتبه کامل گوییم، هرگاه:
$$\text{Rank}(A) = \min(m, n).$$

تعریف ۱.۱.۱۵. اعمال زیر را روی ماتریس A، اعمال سطری مقدماتی می‌نامند:

۱) ضرب یک سطر غیرصفر A در یک اسکالر ناصفر.

۲) تعویض جای دو سطر A با یکدیگر.

۳) افزودن مضربی از یک سطر A به سطر دیگر.

تعریف ۱.۱.۱۶. ماتریس A از مرتبه $m \times n$ را تحویل شده سطری می‌نامیم، هرگاه:

۱) اولین درایه غیرصفر هر سطر، برابر یک باشد.

۲) در هر ستونی که اولین درایه غیرصفر سطر موجود است، سایر درایه‌ها صفر باشند.

تعریف ۱.۱.۱۷. ماتریس R از مرتبه $m \times n$ را تحویل شده سطری پلکانی می‌نامیم، هرگاه:

۱) R تحویل شده سطری باشد.

۲) سطرهای صفر R زیر تمام سطرهای غیرصفر قرار گیرند.

۳) اگر اولین درایه غیرصفر سطر iام در ستون k_iام، $(i = ۱, ۲, \ldots, r)$ واقع باشد و R شامل سطر غیرصفر باشد، آن‌گاه $k_۱ < k_۲ < \ldots < k_r$.

مثال ۱.۱.۱۸. رتبه ماتریس

$$B=\begin{pmatrix} 0 & 1 & 0 & \frac{1}{3} \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

به‌صورت زیر به‌دست می‌آید:
ابتدا با اعمال سطری مقدماتی، ماتریس B را به یک ماتریس تحویل شده سطری پلکانی مانند R تبدیل می‌کنیم، سپس تعداد سطرهای غیر صفر ماتریس R، برابر رتبه ماتریس B است:

$$R=\begin{pmatrix} 0 & 1 & 0 & \frac{-1}{3} \\ 0 & 0 & 1 & \frac{-1}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix} \Longrightarrow \begin{pmatrix} 0 & 3 & 0 & -1 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Longrightarrow B=\begin{pmatrix} 0 & 1 & 0 & \frac{1}{3} \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

بنابراین $\operatorname{rank}(B)=2$.

۲.۱ فضای برداری متناهی روی میدان متناهی گالوا

در این بخش یک فضای برداری را روی میدان متناهی $GF(q)$، که نقش مهمی در نظریه کدگذاری دارد، معرفی می‌کنیم.

تعریف ۱.۲.۱. فرض کنید n یک عدد صحیح و مثبت باشد، دنباله‌ی دلخواه v با n عضو را به‌صورت $v=(v_0,v_1,\ldots,v_{n-1})$ در نظر بگیرید که هر عضو v_i از آن برای $0\le i<n$، یک عضو از میدان متناهی $GF(q)$ است. این دنباله‌ی دلخواه را یک n-تایی روی $GF(q)$ می‌نامیم.
از آن‌جایی که هر عضو v_i می‌تواند هر یک از q عضو $GF(q)$ باشد، درنتیجه q^n، n-تایی متمایز روی $GF(q)$ وجود دارد. مجموعه‌ی این q^n، n-تایی متمایز را با V_n یا $V(n,q)$ نمایش می‌دهیم.

تعریف ۲.۲.۱. مجموع دو n-تایی $v=(v_0,v_1,\ldots,v_{n-1})$ و $u=(u_0,u_1,\ldots,u_{n-1})$ روی $GF(q)$ را به‌صورت زیر تعریف می‌کنیم:

$$u+v=(u_0,u_1,\ldots,u_{n-1})+(v_0,v_1,\ldots,v_{n-1})=(u_0+v_0,u_1+v_1,\ldots,u_{n-1}+v_{n-1}), \quad (2.1)$$

که هر u_i+v_i برای $0\le i<n$، تحت جمع روی $GF(q)$ محاسبه می‌شود، بنابراین عضوی از $GF(q)$ هستند. درنتیجه جمع هر دو n-تایی روی $GF(q)$ یک n-تایی در آن است، پس V_n تحت جمع تعریف شده در (۲.۱) بسته است. هم‌چنین V_n تحت این جمع تعریف شده یک گروه تعویض پذیر است، زیرا عمل جمع روی $GF(q)$ شرکت پذیر و تعویض پذیر است.

عضو صفر از $GF(q)$ را در نظر بگیرید، n-تایی $(0,0,\ldots,0)=0$، عضو همانی از V_n تحت جمع است زیرا:

$$(0,0,\ldots,0)+(v_0,v_1,\ldots,v_{n-1})=(0+v_0,0+v_1,\ldots,0+v_{n-1})=(v_0,v_1,\ldots,v_{n-1}),$$

و

$$(v_0,v_1,\ldots,v_{n-1})+(0,0,\ldots,0)=(v_0+0,v_1+0,\ldots,v_{n-1}+0)=(v_0,v_1,\ldots,v_{n-1}).$$

حال n ‐تایی $v = (v_۰, v_۱, \dots, v_{n-۱})$ را در V_n در نظر بگیرید، برای $۰ \leq i < n$، فرض کنید $-v_i$ وارون جمعی عضو v_i متعلق به میدان $GF(q)$ باشد، بنابراین n ‐تایی $-v = (-v_۰, -v_۱, \dots, -v_{n-۱})$ در V_n، وارون جمعی $v = (v_۰, v_۱, \dots, v_{n-۱})$ است زیرا $v+(-v) = (-v)+v = ۰$؛ بنابراین هر n ‐تایی در V_n دارای معکوس (وارون) جمعی، تحت جمع دو n ‐تایی روی $GF(q)$ است. بنابراین V_n تحت عمل جمع تعریف شده در (۲.۱)، در تمام شرایط گروه تعویض پذیر صدق می‌کند، درنتیجه می‌توان گفت V_n یک گروه تعویض پذیر است.

تعریف ۳.۲.۱. ضرب اسکالر یک n ‐تایی $v = (v_۰, v_۱, \dots, v_{n-۱})$ را در یک عضو c از میدان $GF(q)$، به‌صورت زیر تعریف می‌کنیم:

$$cv = c.(v_۰, v_۱, \dots, v_{n-۱}) = (cv_۰, cv_۱, \dots, cv_{n-۱}), \tag{۳.۱}$$

به‌طوری که هر cv_i برای $۰ \leq i < n$، با ضرب روی میدان $GF(q)$ محاسبه می‌شود.

از آن‌جایی که هر مولفه‌ی cv_i از دنباله‌ی دلخواه cv در (۳.۱) عضوی در میدان $GF(q)$ است، پس $cv = (cv_۰, cv_۱, \dots, cv_{n-۱})$ یک n ‐تایی در V_n است، حال اگر $c = ۱$ فرض شود، آن‌گاه $۱v = v$. پس دیدیم که جمع دو n ‐تایی روی $GF(q)$ و ضرب اسکالر یک n ‐تایی در یک عضو از $GF(q)$، با روابط (۲.۱) و (۳.۱) به‌ترتیب در شرایط شرکت پذیری و پخش پذیری صادق اند، بنابراین V_n یک فضای برداری روی $GF(q)$ است و تمام n ‐تایی‌ها روی $GF(q)$ به‌عنوان بردارهایی از این فضای برداری هستند.

قضیه ۴.۲.۱. *اگر p یک عدد اول و n یک مقدار صحیح و مثبت باشد، آن‌گاه دقیقاً یک میدان متناهی (میدان گالوا) از اندازه‌ی $q = p^n$ وجود دارد که آن را با $GF(q)$ یا F_q نمایش می‌دهیم.*
هم‌چنین تمام میدان‌های متناهی، دارای اندازه‌ی $q = p^n$ برای مقدار p اول و عدد صحیح و مثبت n هستند.

برهان. به مرجع [۸] بخش ۲.۳.۲ مراجعه شود. □

۱.۲.۱ پایه‌ای از فضای برداری V_n

تعریف ۵.۲.۱. بردارهای n ‐تایی زیر را روی $GF(q)$ در نظر بگیرید:

$$\begin{aligned} e_۰ &= (۱, ۰, \dots, ۰), \\ e_۱ &= (۰, ۱, \dots, ۰), \\ &\vdots \\ e_{n-۱} &= (۰, ۰, \dots, ۰, ۱). \end{aligned} \tag{۴.۱}$$

هر n ‐تایی e_i برای $۰ \leq i < n$، تنها یک عضو غیرصفر در مکان iام دارد، که این مولفه‌ی ناصفر، عضو همانی میدان $GF(q)$ است. هر n ‐تایی $v = (v_۰, v_۱, \dots, v_{n-۱})$ روی میدان $GF(q)$ را می‌توان به‌صورت ترکیب خطی از $e_۰$، $e_۱$، ...، $e_{n-۱}$ به شکل زیر نوشت:

$$v = v_۰e_۰ + v_۱e_۱ + \dots + v_{n-۱}e_{n-۱}. \tag{۵.۱}$$

بنابراین $e_\circ$، e_1، $\dots$، e_{n-1} فضای برداری V_n شامل تمام q^n، n -تایی‌ها روی $GF(q)$ را تولید می‌کنند، واضح است که ترکیب خطی داده شده در (۵.۱) برابر بردار صفر است اگر وتنها اگر $v_\circ$، v_1، $\dots$، v_{n-1} همگی برابر صفر باشند، بنابراین e_i ها برای $\circ \leq i < n$، مستقل خطی هستند و تشکیل یک پایه برای V_n می‌دهند.

تعریف ۶.۲.۱. برای $\circ \leq k \leq n$، فرض کنید v_1، $\dots$، v_k، n -تایی‌های مستقل خطی در V_n باشند، آن‌گاه مجموعه‌ی S شامل q^k ترکیب خطی از v_1، $\dots$، v_k به شکل زیر

$$S = \{c_1v_1 + c_2v_2 + \dots + c_kv_k | c_1, \dots, c_k \in F_q\},$$

تشکیل یک زیرفضای k -بعدی از V_n را می‌دهند.

رایج‌ترین فضای برداری مورد استفاده در نظریه‌ی کدگذاری کنترل خطا، فضای برداری $V(n, 2)$ از تمام 2^n -تایی‌ها روی میدان دوتایی $GF(2)$ است، در این حالت n -تایی‌های روی $GF(2)$ را، n -تایی‌های دودویی (باینری) می‌نامند و عمل جمع روی میدان، به پیمانه‌ی دو می‌باشد؛ هم‌چنین در $GF(2)$ وارون عضو همانی یک، خودش است.

مثال ۷.۲.۱. فرض کنید $n = 4$، فضای برداری V_4 از تمام ۴-تایی‌ها روی $GF(2)$، شامل شانزده چهارتایی دودویی به‌صورت زیر است:

$$(1000), (1100), (0110), (1011),$$
$$(0100), (1001), (0011), (1101),$$
$$(0010), (1010), (1110), (1111),$$
$$(0001), (0101), (0111), (0000).$$

هم‌چنین جمع برداری از بردارهایی (۰۱۱۱) و (۱۰۱۱) به‌صورت زیر است:

$$(0111) + (1011) = (0 + 1, 1 + 0, 1 + 1, 1 + 1) = (1100).$$

در مثال بالا چهار بردار (۱۰۰۰)، (۱۱۰۰)، (۱۱۱۰) و (۱۱۱۱) مستقل خطی بوده و تشکیل یک پایه برای V_n می‌دهند، هم‌چنین چهار بردار (۰۰۰۱)، (۰۰۱۰)، (۰۱۱۱) و (۱۱۱۱) مستقل خطی بوده و تشکیل یک پایه‌ی دیگر برای V_n می‌دهند.

تعریف ۸.۲.۱. فرض کنید $u = (u_\circ, \dots, u_{n-1})$ و $v = (v_\circ, \dots, v_{n-1})$ دو n -تایی روی $GF(q)$ باشند، ضرب داخلی u و v به‌صورت زیر است:

$$u.v = u_\circ v_\circ + u_1v_1 + \dots + u_{n-1}v_{n-1} =< u, v >,$$

به‌طوری که اعمال جمع و ضرب روی $GF(q)$ محاسبه می‌شوند. بنابراین ضرب دو n -تایی روی $GF(q)$، یک عضو در $GF(q)$ است، در صورتی که $u.v = \circ$، می‌گوییم u و v برهم عمود هستند.

مثال ۹.۲.۱. ضرب داخلی دو چهارتایی (۱۰۱۱) و (۱۱۰۱) از مثال (۷.۲.۱)، به‌صورت زیر است:

$$(1011).(1101) = 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 1 + 1 = 0.$$

تعریف ۱۰.۲.۱. فرض کنید برای $\text{۰} \le k < n$ ، S یک زیرفضای k -بعدی از فضای برداری V_n از تمام n -تایی‌های روی میدان $GF(q)$ باشد و S_d مجموعه‌ای از n -تایی‌ها در V_n باشد به‌طوری که برای هر u در S و v در S_d، داشته باشیم $u \cdot v = \text{۰}$ یعنی

$$S_d = \{v \in V_n : u \cdot v = \text{۰}, u \in S\}. \qquad (\text{۶.۱})$$

از آن‌جایی که $\text{۰} \cdot u = \text{۰}$، برای هر $u \in S$، S_d شامل n -تایی تمام صفر، از V_n است و درنتیجه غیرتهی است، حال فرض کنید v و w دو عضو از S_d باشند و u نیز یک n -تایی در S باشد، طبق قانون پخش‌پذیری ضرب داخلی داریم:

$$u \cdot (v + w) = u \cdot v + u \cdot w = \text{۰} + \text{۰} = \text{۰},$$

بنابراین $v + w$ نیز متعلق به S_d است و طبق قانون شرکت‌پذیری ضرب داخلی، برای هر اسکالر a در میدان $GF(q)$ و هر n -تایی v و u به‌ترتیب در S_d و S داریم:

$$(a \cdot v) \cdot u = a \cdot (u \cdot v) = a \cdot \text{۰} = \text{۰}.$$

پس $a \cdot v$ نیز متعلق به S_d است، بنابراین S_d در دو شرط زیرفضای یک فضای برداری روی میدان متناهی صادق است، پس S_d یک زیرفضای برداری از فضای برداری V_n شامل تمام n -تایی‌ها روی $GF(q)$ است، S_d را فضای دوگان S می‌نامیم.

قضیه ۱۱.۲.۱. *برای $\text{۰} \le k \le n$ ، فرض کنید S یک زیرفضای k -بعدی از فضای برداری V_n روی میدان $GF(q)$ باشد، بعد فضای دوگان S_d ، $n - k$ است یعنی:*

$$\dim S + \dim S_d = n.$$

برهان. به مرجع [۲۴] قضیه ۲.۰۸ مراجعه شود. □

۳.۱ بخش‌پذیری

تعریف ۱.۳.۱. می‌گوییم a، عدد n را بخش می‌کند، هرگاه عدد صحیحی چون b موجود باشد که $n = ab$. در این‌صورت a را یک بخش‌کننده n، و n را یک مضرب a نامیده و می‌نویسیم $a \mid n$. اگر a یک بخش‌کننده‌ی n نباشد آن‌گاه می‌نویسیم $a \nmid n$.

قضیه ۲.۳.۱.

۱) *اگر $a \mid b$ و $b \mid c$، آن‌گاه* $a \mid c$.

۲) *اگر $a \mid b$، آن‌گاه برای هر c داریم:* $ac \mid bc$.

۳) *اگر $a \mid c$ و $b \mid c$، آن‌گاه برای هر d و e داریم:* $c \mid da + eb$.

۴) *اگر $a \mid b$ و $b \neq \text{۰}$، آن‌گاه* $|a| \le |b|$.

۵) *اگر $a \mid b$ و $b \mid a$، آن‌گاه* $|a| = |b|$.

برهان. به مرجع [۲۶] قضیه ۱.۰۱ مراجعه شود. □

قضیه ۳.۳.۱. *اگر a و b اعداد صحیح باشند و $b > 0$، آن‌گاه اعداد صحیح و منحصر به‌فرد q و r وجود دارند به‌طوری که $a = qb + r$ و $0 \leq r < b$. در واقع $q = \lfloor \frac{a}{b} \rfloor$ و $r = a - bq$.*

برهان. به مرجع [۲۶] قضیه ۱۴۰۱ مراجعه شود.

۴.۱ همنهشتی

گاوس نماد قابل توجهی را معرفی کرد که بسیاری از مسائل بخش‌پذیری اعداد صحیح با آن ساده می‌شوند. وی با این کار شاخه‌ی جدیدی از نظریه‌ی اعداد به‌نام نظریه‌ی همنهشتی‌ها را بنا کرد.

تعریف ۱.۴.۱. فرض می‌کنیم a، b و m اعدادی صحیح هستند و $m > 0$، می‌گوئیم a **همنهشت** b به **هنگ** m است و می‌نویسیم:

$$a \equiv b \pmod{m}, \tag{۷.۱}$$

اگر m تفاضل $a - b$ را بشمارد. عدد m هنگ یا پایه همنهشتی نامیده می‌شود. به‌عبارت دیگر، همنهشتی رابطه‌ی (۲.۱) معادل رابطه‌ی بخش‌پذیری

$$m \mid a - b,$$

است. در حالت خاص، $a \equiv 0 \pmod{m}$ اگر و تنها اگر $m \mid a$. بنابراین $a \equiv b \pmod{m}$ اگر و فقط اگر $a - b \equiv 0 \pmod{m}$.

گاوس علامت همنهشتی را به خاطر تشابه‌اش با علامت تساوی انتخاب کرد. دو قضیه‌ی بعد نشان می‌دهند که همنهشتی‌ها در واقع بسیاری از خواص صوری تساوی‌ها را دارند.

قضیه ۲.۴.۱. همنهشتی *یک رابطه‌ی هم‌ارزی است و داریم:*

۱) $a \equiv a \pmod{m}$ *(انعکاسی).*

۲) $a \equiv b \pmod{m}$ *ایجاب می‌کند که* $b \equiv a \pmod{m}$ *(تقارن).*

۳) $a \equiv b \pmod{m}$ *و* $b \equiv c \pmod{m}$ *ایجاب می‌کنند که* $a \equiv c \pmod{m}$ *(تعدی).*

برهان. به مرجع [۲۶] قضیه ۱۰۵ مراجعه شود. □

قضیه ۳.۴.۱. *هرگاه* $a \equiv b \pmod{m}$ *و* $\alpha \equiv \beta \pmod{m}$*، آن‌گاه*

۱) *به‌ازای هر دو عدد صحیح x و y،* $ax + \alpha y \equiv bx + \beta y \pmod{m}$.

۲) $a\alpha \equiv b\beta \pmod{m}$.

۳) *به‌ازای هر عدد صحیح و مثبت n،* $a^n \equiv b^n \pmod{m}$.

۴) *به‌ازای هر چندجمله‌ای f با ضرایب صحیح،*

$$f(a) \equiv f(b) \pmod{m}.$$

برهان. به مرجع [۲۶] قضیه ۲۰۵ مراجعه شود. □