بسم الله الرحمن الرحيم

دانشکده علوم ریاضی

گروه ریاضی کاربردی

پایان‌نامه کارشناسی ارشد

گرایش کدگذاری

عنوان

کدهای خلوت فاقد دور به طول ۴ بر پایه مجموعه‌های تفاضلی

پژوهشگر

نرگس نکوئی

استاد راهنما

دکتر محمد غلامی

استاد مشاور

دکتر مهدی کدیور

مهر ۱۳۹۲

تقدیم به پدر بزرگوار و مادر مهربانم که:

پیوسته جرعه نوش جام تعلیم و تربیت، فضیلت و انسانیت آن ها بوده ام و همواره لحظات ناب باور بودن، لذت و غرور دانستن، حسارت خواستن، غفلت رسیدن و تمام تجربه های یکتا و زیبای زندگیم، مدیون حضور سبز آن هاست.

تقدم به همسرم که:

سایه مهربانش سایه سار زندگیم می باشد، او که اسوه صبر و تحمل بوده و مشکلات مسیر را برایم تسهیل نمود.

تقدم به یگانه برادرم که:

همواره در طول تحصیل متحمل زحماتم بوده و تکیه گاه من در برابر مشکلات، و وجودش مایه دلگرمی من می باشد.

و تقدیم به خواهرانم که:

وجودشان شادی بخش و صفایشان مایه آرامش من است.

سپاس گزاری...

سپاس خداوندگار حکیم راکه با لطف بی کران خود، آدمی را زیور عقل آراست. بر خود لازم می دانم از همه عزیزانی که در جهت به سرانجام رساندن این مجموعه مرا یاری نمودند، قدردانی نمایم. مراتب قدردانی و سپاس خود را از زحمات بی دریغ استاد با کمالات و شایسته؛ جناب آقای دکتر محمد غلامی ابراز می نمایم، که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه به من دریغ ننمودند و زحمت راهنمایی این پایان نامه را بر عهده گرفتند. از استاد صبور و گرانقدر؛ جناب آقای دکتر مهدی کدیور، که زحمت مطالعه و مشاوره این مجموعه را متقبل شدند، کمال امتنان را دارم، هم چنین از اساتید فرزانه و دلسوز؛ جناب آقای دکتر نقی پور و جناب آقای دکتر رئیسی که زحمت داوری این مجموعه را بر عهده داشتند و از تمامی اساتید محترمی که افتخار شاگردی آنان را داشتم سپاسگزارم.

با آرزوی موفقیت برای تمام عزیزان

نرگس نکویی

مهر ۱۳۹۲

چکیده

در این پایان‌نامه، یک روش کلی برای ساخت کدهای خلوت شبه‌دوری دودویی و غیر دودویی با استفاده از جایگذاری عضوهایی از یک ماتریس روی $F(q)$، با ماتریس‌های خلوتی که ساختار چرخشی دارند، معرفی می‌شود. این ساخت بر پایه مفاهیمی از بردارهای مکان، ماتریس‌های پراکنده و ماتریس‌های پایه است. در ادامه روش‌هایی برای ساخت ماتریس‌های پایه با استفاده از زیرگروه‌های دوری و زیرگروه‌های جمعی از میدان‌های متناهی و $(v, k, ۱)$-مجموعه‌های تفاضلی معرفی می‌شود.

فرض کنید F_q یک میدان با q عضو بوده و $D = \{d_۱, d_۲, \ldots, d_k\}$ یک $(v, k, ۱)$-مجموعه تفاضلی برای Z_v با $d_۱ < d_۲ < \cdots < d_k$ باشد. سه روش ساخت کد تحت شرایط $v = q - ۱$ و $q \geq ۲d_k$ و $q \geq ۲d_{k-۱}$ مطرح می‌شود، به‌طوری که بعضی کدهای منظم فاقد دور به‌طول ۴ را تولید می‌کند. در پایان، نتایج شبیه‌سازی نشان می‌دهد که کدهای ساخته شده بر روی کانال‌های AWGN با الگوریتم کدگشای عبور-پیام و مجموع-حاصل‌ضرب تکراری به‌خوبی عمل می‌کنند.

رده بندی موضوعی ریاضی ۲۰۱۳: 94B60، 94B05، 94B25.

کلمات کلیدی : کدهای خلوت، مجموعه‌های تفاضلی، ماتریس پایه، ماتریس پراکنده، میدان متناهی، بردار مکان.

فهرست مطالب

مقدمه ۴

فهرست نمادها ۶

۱ مقدمات و پیش‌نیازها ۸

۱.۱ ساختارهای جبری ۹

۲.۱ فضاهای برداری روی میدان‌های متناهی ۱۰

۳.۱ همنهشتی ۱۳

۴.۱ گراف ۱۴

۵.۱ طرح‌های ترکیبیاتی ۱۷

۶.۱ رتبه ماتریس ۲۰

۲ کدهای خطی ۲۱

۱.۲ کدهای بلوکی ۲۲

۲.۲ کانال‌های اطلاعات ۲۳

۱.۲.۲ کانال بدون حافظه گسسته ۲۳

۲.۲.۲ کانال دوتایی متقارن (BSC) ۲۳

۳.۲.۲ کانال با اغتشاش گاوسی سفید جمع شونده-ورودی دوتایی(BI – AWGN) ۲۴

۳.۲ کدهای خطی ۲۴

۴.۲ ماتریس مولد و ماتریس بررسی توازن ۲۵

۵.۲ کدهای دوری ۲۸

۶.۲ ماتریس مولد وچندجمله‌ای بررسی ۳۰

۷.۲ کدهای BCH ۳۱

۸.۲ کدهای رید-سولومن ۳۱

۹.۲ کدگشایی کدهای غیر دودویی BCH و RS: الگوریتم برلیکمپ-مسی ۳۲

۱۰.۲ کدهای شبه‌دوری ۳۷

۱۱.۲ کدهای خلوت ۳۹
۱۲.۲ ساختار کدهای خلوت ۳۹
۱۳.۲ نرخ کدهای خلوت ۴۰
۱۴.۲ گراف تنر برای کدهای بلوکی خطی ۴۱
۱۵.۲ کدگشایی کدهای خلوت ۴۲
۱۶.۲ الگوریتم‌های گذرنده پیام و عملکرد گره‌ها ۴۳
۱۷.۲ کدگشایی مجموع-حاصل‌ضرب ۴۵

۳ کدهای خلوت شبه‌دوری دودویی و غیر دودویی بر پایه میدان‌های متناهی ۵۲
۱.۳ بردارهای مکان دودویی و q-تایی ۵۳
۲.۳ ماتریس پراکنده دودویی و q-تایی از عضوهای میدان ۵۳
۳.۳ ماتریس پایه ۵۴
۴.۳ ساخت کدهای خلوت شبه‌دوری دودویی و q-تایی بر پایه میدان‌های متناهی ۵۵
۵.۳ ساخت بر پایه زیرگروه‌های جمعی از میدان‌های متناهی ۵۶
۱.۵.۳ دسته‌ای از کدهای خلوت شبه‌دوری دودویی ۵۷
۲.۵.۳ دسته‌ای از کدهای خلوت شبه‌دوری q-تایی ۵۸
۶.۳ ساخت بر پایه زیر گروه‌های دوری از میدان‌های متناهی ۵۸
۱.۶.۳ دسته‌ای از کدهای خلوت شبه‌دوری دودویی ۶۰
۲.۶.۳ دسته‌ای از کدهای خلوت شبه‌دوری q-تایی ۶۰

۴ کدهای خلوت فاقد دور به طول ۴ بر پایه $(v, k, 1)$-مجموعه‌های تفاضلی ۶۲
۱.۴ یک روش ساخت کلی بر پایه $(v, k, 1)$-مجموعه‌های تفاضلی ۶۳
۲.۴ کدهای خلوت شبه‌دوری غیر دودویی تحت شرط $v = q - 1$ ۶۴
۳.۴ کدهای خلوت شبه‌دوری غیر دودویی تحت شرط $q \geq 2d_k$ ۶۹
۴.۴ کدهای خلوت شبه‌دوری غیر دودویی تحت شرط $q \geq 2d_{k-1}$ ۷۴
۵.۴ ساخت کد و نتایج شبیه‌سازی ۷۷
۶.۴ نتیجه‌گیری ۸۰

مراجع ۸۱

واژه‌نامه فارسی به انگلیسی ۸۳

واژه‌نامه انگلیسی به فارسی ۸۷

Abstract ۹۱

مقدمه

نظریه کدگذاری کانال، یکی از شاخه‌های پرکاربرد مخابرات است که هدف از آن ارسال اطلاعات از فرستنده از طریق یک کانال فیزیکی دارای اغتشاش، به گیرنده می‌باشد. شانون[1] را می‌توان پایه‌گذار این نظریه دانست که در مقاله‌ای اساسی در سال ۱۹۴۸ ثابت نمود کدهای تصحیح کننده خطا با نرخ ارسال کمتر از ظرفیت کانال وجود دارند که پس از ارسال بر روی کانال، دارای احتمال خطای کدگشایی نزدیک به صفر می‌باشند [۱۵]. شانون این مطلب را به‌صورت وجودی اثبات کرد و روند اثبات او بر پایه نظریه احتمال بوده و روش خاصی را جهت معرفی کد مطلوب مشخص نمی‌کرد. پس از آن بود که تلاش‌های زیادی برای رسیدن به کدهای مطلوب آغاز گردید و کدهای معروفی نظیر کدهای BCH ، رید-سولومن[2] و کدهای خلوت یا LDPC مطرح شدند.

کدهای خلوت اولین بار توسط گالاگر[3] در سال ۱۹۶۰ مطرح شدند [۸، ۹]. سپس تنر [4] در سال ۱۹۸۱، یک بیان جدید از کدهای خلوت از نقطه نظر گرافیکی را ارائه کرد. در سال ۱۹۹۰ محققان، تحقیقات خود را در زمینه کدهای روی گراف‌ها و کدگشایی تکراری شروع کردند. این کدها روی کانال‌های انتقال و ذخیره داده دارای کارآیی بسیار نزدیک به نرخ شانون هستند [۱۵].

در این پایان‌نامه میدان متناهی $F(q)$ را در نظر گرفته و مفهوم بردار مکان، ماتریس پایه و ماتریس پراکنده را معرفی می‌کنیم. سپس یک روش کلی برای ساخت کدهای خلوت شبه‌دوری دودوئی و q-تایی با استفاده از جایگذاری عضوهایی از ماتریس پایه روی $F(q)$ با ماتریس پراکنده متناظر با آن، ارائه می‌دهیم. در ادامه روش‌هایی برای ساخت ماتریس‌های پایه با استفاده از زیرگروه‌های دوری و زیرگروه‌های جمعی از میدان‌های متناهی و $(v, k, 1)$-مجموعه‌های تفاضلی معرفی می‌شود.

سه روش ساخت برای کدهای خلوت شبه‌دوری دودویی و q-تایی با استفاده از $(v, k, 1)$-مجموعه‌های تفاضلی $D = \{d_1, d_2, \ldots, d_k\}$ (که در آن $d_1 < d_2 < \cdots < d_k$) تحت شرایط $v = q - 1$، $q \geq 2d_k$ یا $q \geq 2d_{k-1}$ مطرح می‌شود، به‌طوری که بعضی کدهای منظم فاقد دور به‌طول ۴، یعنی کدهایی که کمر گراف متناظر با آن‌ها حداقل برابر با ۶ است، تولید می‌شود. به‌ویژه این کدها تحت کدگشای مجموع حاصل‌ضرب به خوبی عمل می‌کنند. مجموعه‌های تفاضلی برای ساخت کدهای دوری و کدهای خود متعامد نیز استفاده می‌شوند [۲۰، ۲۱].

1. Shannon
2. Reed-Solmon
3. Gallager
4. Tanner

در این پایان‌نامه به‌طور خلاصه:
در فصل اول، مقدمات و تعاریف اولیه مورد نیاز برای فصول آتی را بیان می‌کنیم، که برگرفته از مراجع [۲۳، ۲۴، ۲۵، ۲۶، ۲۸، ۲۹] می‌باشند.
در فصل دوم، ابتدا کدهای خطی را معرفی کرده و در ادامه کدهای دوری و شبه‌دوری را بیان می‌کنیم، سپس ضمن معرفی کدهای خلوت یک قاعده کدگشای مجموع-حاصل‌ضرب از آن را توضیح می‌دهیم. مطالب این فصل برگرفته از [۹، ۱۶، ۲۷] هستند.
در فصل سوم، ابتدا مفهوم بردار مکان، ماتریس پراکنده و ماتریس پایه را توضیح می‌دهیم. سپس یک روش ساخت کلی برای کدهای خلوت شبه‌دوری دودویی و q-تایی را معرفی می‌کنیم. در ادامه روشی برای ساخت ماتریس پایه بر پایه زیرگروه‌های جمعی و زیرگروه‌های دوری از میدان‌های متناهی را معرفی می‌کنیم [۱۷].
در فصل چهارم، سه روش ساخت کدهای خلوت شبه‌دوری دودویی و q-تایی بر پایه $(v,k,1)$-مجموعه‌های تفاضلی، تحت شرایط $v = q-1$، $q \geq 2d_k$ یا $q \geq 2d_{k-1}$ مطرح می‌شود، به‌طوری که این کدها فاقد دور به طول ۴ هستند [۶]. در پایان با استفاده از نتایج شبیه‌سازی نشان می‌دهیم که کدهای ساخته شده بر روی کانال‌های AWGN با الگوریتم کدگشای عبور-پیام مجموع-حاصل‌ضرب تکراری به‌خوبی عمل می‌کنند.

فهرست نمادها

$\emptyset$ مجموعه تهی ۱۰
$\mathbb{Z}$ اعداد صحیح ۱۰
$\forall$ به ازای هر ۱۰
$\in$ تعلق داشتن عضو به مجموعه ۱۰
$\wedge$ و ۱۰
$F(q)$ میدان گالوا از مرتبه q ۱۰
$V(n,q)$ فضای برداری n تایی روی F_q ۱۰
dim بعد فضا ۱۲
$\langle\,\rangle$ ضرب داخلی ۱۲
mod همنهشتی ۱۳
$\equiv$ هنگ ۱۳
$|$ بخش‌پذیری ۱۳
$\perp$ دوگان ۱۳
$\mathbb{Z}_n$ مجموعه اعداد صحیح به پیمانه n ۱۴
T ترانهاده ۱۸
$d(x,y)$ فاصله x از y ۲۲
min می‌نیمم ۲۲
log لگاریتم ۲۲
$\sum$ مجموع ۲۳
$\prod$ حاصل‌ضرب ۲۳
G ماتریس مولد کد ۲۵
H ماتریس بررسی توازن کد ۲۵
$\lfloor\,\rfloor$ جزء صحیح ۲۶
$\exists$ وجود دارد ۲۷
deg درجه ۲۸

rank(A) رتبه ماتریس A ۴۱
$\det(A)$ دترمینان ماتریسA ۶۴
$\Longleftrightarrow$ اگر و تنها اگر ۶۴

فصل ۱

مقدمات و پیش‌نیازها

اهداف کلی فصل

در این فصل به بیان مفاهیم گروه، حلقه، میدان متناهی، فضای برداری، همنهشتی و قضایایی می‌پردازیم که در فصول آتی پایان‌نامه از آن‌ها استفاده می‌کنیم. در ادامه به معرفی برخی طرح‌های ترکیبیاتی پرداخته و در پایان فصل تعاریفی از گراف، ماتریس جایگشتی چرخشی و رتبه ماتریس را ارائه می‌دهیم. لازم به ذکر است که مطالب این فصل برگرفته از [۲۳، ۲۴، ۲۵، ۲۶، ۲۸، ۲۹] می‌باشد.

۱.۱ ساختارهای جبری

تعریف ۱.۱.۱. فرض کنید G مجموعه‌ای ناتهی باشد. یک تابع از $G \times G$ به G را یک عمل دوتایی روی G گوییم.

تعریف ۲.۱.۱. مجموعه ناتهی G را به همراه عمل دوتایی $*$ یک **گروه** می‌نامیم، هرگاه:

۱) به ازای هر $a, b, c \in G$، $(a * b) * c = a * (b * c)$، یعنی عمل $*$ شرکت‌پذیر باشد.

۲) عضو $e \in G$ وجود داشته باشد که به ازای هر $a \in G$، $a * e = e * a = a$. e را عضو همانی یا عضو بی‌اثر گوییم.

۳) به ازای هر $a \in G$ عضو $a^{-1} \in G$ وجود داشته باشد به‌طوری که $a * a^{-1} = a^{-1} * a = e$. a^{-1} را وارون a گوییم.

تعریف ۳.۱.۱. اگر به ازای هر $a, b \in G$ داشته باشیم $a * b = b * a$، گوییم گروه G تعویض‌پذیر یا آبلی است.

تعریف ۴.۱.۱. اگر G یک گروه متناهی باشد، آنگاه $|G|$، یعنی مرتبه G عبارت است از تعداد اعضای G.

تعریف ۵.۱.۱. زیرمجموعه H از گروه G یک زیرگروه G است اگر و تنها اگر:

۱) H تحت عمل G بسته باشد؛

۲) عضو همانی e از G به H تعلق داشته باشد؛

۳) برای هر a از H عضو a^{-1} به H نیز تعلق داشته باشد.

تعریف ۶.۱.۱. مجموعه ناتهی R را همراه با دو عمل شرکت‌پذیر "+" (بنام جمع) و "." (بنام ضرب) روی آن یک **حلقه** نامیده و با علامت $(R, +, .)$، نمایش می‌دهیم هرگاه:

۱) $(R, +)$ به همراه عمل جمع یک گروه آبلی باشد. عضو بی‌اثر $(R, +)$ را با علامت $\circ$ نمایش می‌دهیم.

۲) قوانین توزیع‌پذیری برقرار باشند، یعنی برای هر $a, b, c \in R$،

$$a.(b + c) = (a.b) + (a.c), \quad (b + c).a = (b.a) + (c.a).$$

تعریف ۷.۱.۱. حلقه R را تعویض‌پذیر گوییم، هرگاه عمل ضرب در R تعویض‌پذیر باشد، یعنی به ازای هر $a, b \in R$ داشته باشیم $a.b = b.a$.

تعریف ۸.۱.۱. حلقه R را یک‌دار گوییم هرگاه عضو همانی ضربی داشته باشد.

اعداد صحیح $\mathbb{Z}$ بهترین مثال شناخته‌شده از یک حلقه می‌باشد.

تعریف ۹.۱.۱. زیرمجموعه T از حلقه R، یک زیر حلقه از R نامیده می‌شود، اگر با اعمال تعریف شده در R، خود یک حلقه باشد.

تعریف ۱۰.۱.۱. اگر $(R,+,.)$ یک حلقه باشد و $\emptyset \neq S \subseteq R$ آن‌گاه S یک ایده‌آل نامیده می‌شود، اگر:

۱) $\forall_{a\in S}\forall_{b\in S}[a-b\in S]$

۲) $\forall_{a\in S}\forall_{b\in R}[ab\in S \wedge ba\in S]$

روشن است که اگر S یک ایده آل در R باشد، آن‌گاه $(S,+,.)$ یک زیرحلقه می‌باشد.

تعریف ۱۱.۱.۱. میدان حلقه‌ای جابجایی است که عناصر ناصفر آن تحت عمل ضرب تشکیل یک گروه می‌دهند.

تعریف ۱۲.۱.۱. یک میدان متناهی عبارت است از، میدانی که تعداد عناصر آن متناهی باشند. این تعداد را مرتبه میدان می‌نامند.

قضیه اساسی زیر در مورد میدان متناهی توسط گالوا [1] (ریاضیدان فرانسوی) ثابت شده است.

قضیه ۱۳.۱.۱. *به ازای هر عدد اول p و هر عدد طبیعی n میدانی با p^n عضو وجود دارد و به‌علاوه هر دو میدان با p^n عضو یکریخت‌اند.*

برهان. به مرجع [۲۶] قضیه ۲۰۲ مراجعه شود. □

تعریف ۱۴.۱.۱. اگر p عدد اول و n عدد طبیعی باشد، آن‌گاه میدان منحصر به فرد $q=p^n$ عضوی را میدان گالوا نامیده و با $GF(q)$ یا F_q نمایش می‌دهیم.

تعریف ۱۵.۱.۱. فرض کنید a یک عنصر ناصفر از میدان F_q باشد. کوچکترین عدد صحیح مثبت n به‌طوری که $a^n=1$، مرتبه a نامیده می‌شود.

تعریف ۱۶.۱.۱. یک عنصر ناصفر $a\in F_q$ را عنصر اولیه میدان نامند هرگاه، مرتبه a برابر با $q-1$ باشد، به‌طوری که عناصر ناصفر میدان دقیقاً $1, a, \ldots, a^{q-2}$ با $a^{q-1}=1$ هستند.

۲.۱ فضاهای برداری روی میدان‌های متناهی

تعریف ۱.۲.۱. فرض می‌کنیم که q توانی از یک عدد اول و F_q میدان متناهی از مرتبه q باشد. عناصر F_q اسکالرها نامیده خواهند شد. مجموعه F_q^n، شامل همه n-تاییهای مرتب بر F_q را با $V(n,q)$ نمایش می‌دهیم و عناصرش را بردار می‌نامیم. دو عمل بر $V(n,q)$ تعریف می‌کنیم:

1. Galois

(۱) جمع بردارها: اگر $X = (x_۱, x_۲, \ldots, x_n)$ و $Y = (y_۱, y_۲, \ldots, y_n)$ دو بردار در $V(n,q)$ باشند، آنگاه

$$X + Y = (x_۱ + y_۱, x_۲ + y_۲, \ldots, x_n + y_n)$$

(۲) ضرب یک بردار در یک اسکالر: اگر

$$X = (x_۱, x_۲, \ldots, x_n) \in V(n,q) \quad و \quad a \in F_q,$$

آن‌گاه $aX = (ax_۱, ax_۲, \ldots, ax_n)$.

$V(n,q)$، همراه با دو عمل بالا یک **فضای برداری** روی F_q تشکیل می‌دهد، هرگاه برای هر u، v، و w در $V(n,q)$ و برای هر a و b در F_q، داشته باشیم:

(۱) $u + v \in V(n,q)$.

(۲) $(u + v) + w = u + (v + w)$.

(۳) بردار صفر $۰ = (۰, ۰, \ldots, ۰)$ متعلق به $V(n,q)$ است و در شرط $u + ۰ = ۰ + u = u$ صدق می‌کند.

(۴) برای عنصر $u = (u_۱, u_۲, \ldots, u_n) \in V(n,q)$، عنصر $-u = (-u_۱, -u_۲, \ldots, -u_n)$، هم‌چنین در شرط $u + (-u) = ۰$ صدق می‌کند.

(۵) $u + v = v + u$.

(خواص (۴) – (۱) بدین معنی است که $V(n,q)$، تحت عمل جمع، یک گروه آبلی است)

(۶) (بسته بودن تحت ضرب اسکالر) $av \in V(n,q)$.

(۷) (قوانین توزیع‌پذیری) $(a + b)u = au + bu$، $a(u + v) = au + av$.

(۸) $(ab)u = a(bu)$.

(۹) $۱u = u$، جائیکه ۱ همانی ضربی F_q است.

قضیه ۲.۲.۱. *زیرمجموعه غیر تهی C از $V(n,q)$ یک زیرفضا است اگر و تنها اگر C تحت جمع و ضرب اسکالر $V(n,q)$ بسته باشد، یعنی اگر و تنها اگر C در دو شرط زیر صدق کند:*

۱) *اگر $x, y \in C$، آنگاه $x + y \in C$.*

۲) *اگر $a \in F_q$ و $x \in C$ آنگاه $ax \in C$.*

برهان. به مرجع [۲۹] قضیه ۱۰۴ مراجعه شود. □

تعریف ۳.۲.۱. فرض کنید $V(n,q)$ یک فضای برداری روی F_q باشد. یک ترکیب خطی از بردارهای $v_۱, v_۲, \ldots, v_r \in V(n,q)$، برداری است به شکل $\lambda_۱v_۱ + \lambda_۲v_۲ + \ldots, \lambda_r v_r \in V(n,q)$ که $\lambda_۱, \ldots, \lambda_r \in F_q$، اسکالر می‌باشند.

تعریف ۴.۲.۱. فرض کنیم $V(n,q)$ فضای برداری روی F_q باشد. یک زیرمجموعه S از $V(n,q)$ وابسته خطی نامیده می‌شود هرگاه بردارهایی متمایز مانند $\alpha_1, \alpha_2, \ldots, \alpha_n$ در S و اسکالرهایی مانند $c_1, c_2, \ldots, c_n$ که همگی صفر نباشند در F_q یافت شود، به‌طوری که

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n = 0.$$

مجموعه‌ای که وابستهٔ خطی نباشد مستقل خطی نام دارد.

گزاره ۵.۲.۱. *فرض کنیم V یک فضای برداری با بعد متناهی باشد، و بعد V برابر با n باشد، در این صورت*

۱) *هر زیرمجموعهٔ V که شامل بیش از n بردار باشد وابستهٔ خطی است.*

۲) *هیچ زیرمجموعه‌ای از V که کمتر از n بردار داشته باشد نمی‌تواند V را پدید آورد.*

برهان. به مرجع [۲۸] صفحه ۶۱ مراجعه شود. □

تعریف ۶.۲.۱. فرض کنید S یک زیرفضای برداری $V(n,q)$ باشد. در این‌صورت زیرمجموعه‌ای از S مانند $\{v_1, v_2, ..., v_r\}$ یک مجموعهٔ مولد (یا مجموعه سازنده) S نامیده می‌شود اگر هر بردار در S را بتوان به‌صورت یک ترکیب خطی از $v_r, v_2, \ldots, v_1$ بیان کرد.

تعریف ۷.۲.۱. فرض کنیم $V(n,q)$ فضای برداری باشد. یک پایه برای $V(n,q)$، مجموعه‌ای مستقل خطی از بردارهای $V(n,q)$ است که فضای $V(n,q)$ را پدید آورد. فضای $V(n,q)$ دارای بعد متناهی است هرگاه یک پایه متناهی داشته باشد.

قضیه ۸.۲.۱. *فرض کنید $\{v_1, v_2, \ldots, v_k\}$ یک پایه زیرفضای S از $V(n,q)$ باشد. در این‌صورت*

۱) *هر بردار S می‌تواند به صورت ترکیب خطی یکتایی از بردارهای پایه بیان گردد.*

۲) *S شامل دقیقاً q^k بردار است.*

برهان. به مرجع [۲۹] قضیه ۳۰۴ مراجعه شود. □

از قضیه (۸.۲.۱) نتیجه می‌شود که هر دو پایه یک زیرفضای برداری S دارای تعداد برابر k بردار می‌باشند، جائیکه $|S| = q^k$. عدد k بعد فضای S نامیده می‌شود و به‌صورت $\dim(S)$ نمایش داده می‌شود.

تعریف ۹.۲.۱. فرض کنید $v = (v_1, \ldots, v_n)$، و $w = (w_1, \ldots, w_n)$، بردارهایی در F_q^n باشند:

(۱) ضرب داخلی v و w، به‌صورت زیر تعریف می‌شود:

$$< v, w > := v_1w_1 + \ldots + v_nw_n \in F_q.$$

(۲) دو بردار v و w را متعامد گوییم هرگاه، $v.w = 0$.

(۳) اگر S یک زیر مجموعه ناتهی از F_q^n باشد، دوگان S با $S^\perp$ نمایش داده، و به‌صورت زیر تعریف می‌شود:

$$S^\perp = \{v \in F_q^n : v.s = ۰ \quad \forall s \in S\}.$$

هر گاه $S = \phi$، در این‌صورت تعریف می‌کنیم: $S^\perp = F_q^n$.

قضیه ۱۰.۲.۱. *هر گاه S یک زیر مجموعه F_q^n باشد، در این‌صورت:*

$$\dim(\mathrm{S}) + \dim(\mathrm{S}^\perp) = n.$$

برهان. به مرجع [۲۸] صفحه ۱۳۴ مراجعه شود. □

۳.۱ همنهشتی

گاوس [1] 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 ۱.۳.۱. فرض کنیم a، b و m اعدادی صحیح باشند و $m > ۰$. گوئیم a **همنهشت** b به **هنگ** m است و می‌نویسیم:

$$a \equiv b \pmod{m}, \tag{۱.۱}$$

اگر m تفاضل $a - b$ را بشمارد. عدد m **هنگ** همنهشتی نامیده می‌شود. به‌عبارت دیگر، همنهشتی رابطه‌ی (۱.۱) معادل رابطه‌ی بخش‌پذیری

$$m \mid (a - b)$$

است. در حالت خاص، $a \equiv ۰ \pmod{m}$ اگر و تنها اگر $m \mid a$. بنابراین، $a \equiv b \pmod{m}$ اگر و تنها اگر $a - b \equiv ۰ \pmod{m}$.

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

قضیه ۲.۳.۱. *همنهشتی یک رابطه‌ی هم‌ارزی است. یعنی، 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 [۲۳] قضیه ۱۰۵ مراجعه شود. □

1. Gauss