دانشکده علوم

گروه ریاضی

پایان نامه کارشناسی‌ارشد رشته‌ی ریاضی کاربردی

عنوان پایان نامه :

کدهای ثابت دوری از طول P^s روی حلقه $R = F_{p^m} + uF_{p^m}$

استاد راهنما :

دکترمهرداد احمدزاده

نگارش:

شهیر اسحاقی

بهمن ماه ۱۳۹۰

بسم الله الرحمن الرحيم

کلیه حقوق مادی مترتب بر نتایج مطالعات، ابتکارات و نوآوری های ناشی از تحقیق موضوع این پایان نامه متعلق به دانشگاه رازی است.

قدردانی و تشکر

پس از شکر و ستایش خدای متعال، سپاسگذاری و امتنان قلبی خویش را نسبت به جناب آقای دکتر **مهرداد احمدزاده**، که در مدت تحصیل و مراحل تدوین این پایان نامه راهنما و راهگشای مشکلات بنده بودند، ابراز می دارم.

همچنین از زحمات اساتید ارجمند جناب آقای **دکتر بهروز عدالت زاده** و جناب آقای **دکتر بیژن طائری** که بذل محبت فرموده و زحمت داوری داخلی و خارجی این پایان نامه را پذیرفتند صمیمانه تقدیر و تشکر می کنم.
و از کلیه اساتید گروه ریاضی از جمله **دکتر ابوالقاسمی** ، **دکتر فرج زاده**، **دکتر امینی**، **دکتر درویشی** که در مدت تحصیل از محضر علم و ادبشان بسیار استفاده نموده ام، کمال تشکر و قدردانی را دارم.

لازم می دانم از خانم **زهرا فرامانی** بابت تمامی زحمات و راهنمایی هایشان در طول دوران تحصیلم تشکر وسپاسگذاری کنم.

در پایان از کلیه دانشجویان ارشد گروه ریاضی، بخصوص آقای **محمد امین امیدی**، آقای **محمود قبادی**، آقای **سعید رستمی کیا**،آقای **محسن اکبری**،**منصور فتاحی**،آقای **اردشیرکرمیان** وآقای **خسرو مهرابی**،آقای **مجید مهری**،آقای **نورالله درویشی**،آقای **جعفر مرادی**، صمیمانه تشکر می‌کنم و موفقیت روزافزونشان را از خداوند متعال خواستارم.

تقدیم به :

پدر و مادرم

چکیده

کدهای پایادوری نقش ویژه‌ای را در نظریه‌ی کدهای تصحیح کننده‌ی خطا[1] بازی می‌کنند. مهمترین نوع از این کدها، کدهای دوری هستند. در این پایان نامه پس از بیان مقدماتی از جبر، قواعد و فواصل همینگ برای کدهای منفی دوری که نوع خاصی از کدهای پایادوری هستند بیان می‌شوند. در ادامه کدهای پایادوری را روی حلقه $R = F_{p^m} + uF_{p^m}$ معرفی می‌کنیم،که در آن $F_q = F_{p^m}$ از مرتبه q است و u متغیر است. سپس قواعد و فواصل همینگ تمامی $\alpha + u\beta$ -کدهای پایادوری را بیان می‌کنیم. همچنین‌کدهای دوری را روی حلقه $R = F_{p^m} + uF_{p^m}$ بررسی کرده ودر خاتمه نیز با استفاده از یک یکریختی حلقه‌ای، تناظری یک به‌یک بین کدهای دوری وکدهای پایادوری ایجاد می‌کنیم که تمامی خواص کدهای دوری را به کدهای پایادوری منتقل می‌کند.

[1] *Error Correcting Codes*

فهرست مندرجات

پیشگفتار

کدهای دوری با استفاده از یک تعریف انتقال‌دوری، بیان می‌شوند. هر کدواژه‌ی $(c_0, c_1, \ldots, c_{n-1})$ با چندجمله‌ای

$$c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1},$$

در $R_n[x]$ متناظر می‌شود، که در آن $R_n[x]$ حلقه‌ی چندجمله‌ایهای x به پیمانه $x^n - 1$ است. یک انتقال-دوری از هر کدواژه نیز با حاصلضرب x در چندجمله‌ای متناظر کدواژه حاصل می‌شود.

بیشتر تحقیقاتی که در زمینه‌ی کدهای دوری انجام شده است، در شرایطی انجام شده است که طول کد یا همان n، نسبت به مشخصه‌ی میدان F اول باشد.

تمامی λ - کدهای ثابت دوری تحت عنوان ایده‌آلهای $\langle f(x) \rangle$ از $\frac{F_q[x]}{\langle x^n - \lambda \rangle}$ دسته بندی می‌شوند، که در آن $f(x)$ یک عامل یا شمارنده $x^n - \lambda$ است. در اینجا q به صورت توانی از p است که مشخصه میدان است. در حالتی که طول کد یا n بر مشخصه‌میدان یا p بخش پذیر باشد ، تعریف ریشه تکراری کدها را خواهیم داشت. نخستین بار ریشه‌های تکراری توسط برمن[2] [4] در سال 1967 و سپس در سالهای 1970 و 1980 توسط نویسندگانی چون ماسی[3] [18] و فالکنر[4] [13] و روث[5] و سریوسی[6] [23] مطالعه شد. همچنین این مطلب به طور وسیعی توسط کاستاگنولی[7] [9] و ون لینت[8] [28] بررسی شدند. در این پایان‌نامه نیز با این دیدکه طول کدواژه ی c یا همان n بر مشخصه‌ی میدان بخش پذیر است،کدهای ثابت دوری روی حلقه‌ی $R = F_{p^m} + uF_{p^m}$ بررسی می‌شوند. هدف این پایان نامه بررسی تمامی کدهای ثابت دوری از طول p^s روی $F_{p^m} + uF_{p^m}$ است.

فصل اول این پایان نامه تعاریف و قضایایی از جبر و معرفی کدهای خطی را بیان می‌کند.

---

[2] *Berman*
[3] *Massey*
[4] *Falkner*
[5] *Roth*
[6] *Seroussi*
[7] *Castagnoli*
[8] *Vanlint*

در فصل دوم مبحث کدهای منفی‌دوری و فواصل همینگ آنها بیان می‌شوند. این فصل برگرفته از مقاله [11] است.فصل سوم این تحت عنوان کدهای ثابت دوری بعنوان توسیعی ازکدهای منفی‌دوری برگرفته ازمقاله [1] است. در این فصل سوم کدهای ثابت دوری و کدهای‌دوری و انواع این کدها بررسی و بیان خواهند گردید.

فصل اول

مباحث و تعاریف مقدماتی

در این فصل مفاهیم ابتدا مفاهیمی ازجبر را بیان کرده، و در ادامه به معرفی کدهای خطی می پردازیم.

۱.۱ حلقه [۹] و میدان [۱۰]

تعریف ۱. 1.1 : مجموعه غیرتهی G با عمل دوتایی $*$ یک گروه[۱۱] نامیده می شود، هرگاه:

۱) مجموعه G نسبت به $*$ بسته باشد، یعنی $\forall\ x,y\ \in G\ ;\ x*y\ \in G$.

۲) عمل $*$ در G شرکت‌پذیر باشد، یعنی $\forall\ x,y,z\ \in G\ ;\ x*(y*z)=(x*y)*z$.

۳) مجموعه G دارای عضوی مانند e باشد، بطوریکه $\forall\ x\in G,\ x*e=e*x=x$.

۴) برای هر $x\in G$ عضوی مانند $y\in G$ وجود داشته باشد، بطوریکه $x*y=y*x=e$. به y وارون[۱۲] x می‌گوییم.

اگر G فقط بسته و شرکت‌پذیر باشد، آنگاه G نیم‌گروه[۱۳] نامیده می‌شود.

همچنین اگر $\forall\ x,y\ \in G$ داشته باشیم $x*y=y*x$، آنگاه G را یک گروه آبلی[۱۴] می‌گوییم.

[9] *Ring*
[10] *Field*
[11] *Group*
[12] *Inverse*
[13] *Semi group*
[14] *Abelian*

تعریف 1. 1. 2 : فرض کنید G یک گروه باشد. هر زیرمجموعه غیرتهی مانند H از G را یک زیرگروه[۱۵] از G می‌نامیم، هرگاه H تحت عمل G خود یک گروه باشد. در صورتی که H زیرگروه G باشد آنرا با $H \leq G$ نشان می‌دهیم.

در اینجا به معرفی مفهوم حلقه می پردازیم:

تعریف 1. 1. 3 : فرض‌کنیم R مجموعه‌ای ناتهی باشد. اعمال دوتایی $+ , \times$ را روی R در نظر می‌گیریم. دستگاه $(R , + , \times)$ یک حلقه نامیده می شود، هرگاه:

۱) $(R , +)$ یک گروه آبلی باشد.

۲) $(R , \times)$ یک نیم‌گروه باشد.

۳) ضرب روی جمع خاصیت توزیع پذیری داشته باشد. به عبارت دیگر

$$\forall\, a, b, c \in R \quad ; \quad a.(b + c) = ab + ac \quad , \qquad (b + c)a = ba + ca.$$

اگر تعداد اعضای حلقه‌ی R متناهی[۱۶] باشد، آنرا حلقه‌ی متناهی می‌گوییم. تعداد اعضای R را مرتبه[۱۷] حلقه نامیده و با $|R|$ نشان می‌دهیم.

مثال 1. 1. 4: مجموعه اعدادصحیح با عمل جمع و ضرب معمولی اعداد یک حلقه است.

تعریف 1. 1. 5 : اگر نیم‌گروه $(R,\times)$ در حلقه‌ی $(R , + , \times)$ دارای عضو خنثی باشد،آنگاه حلقه‌ی R را یکدار می‌نامیم. یعنی

$$\forall \; a \in R \; ; \; a.1_R = 1_R.a = a.$$

که در اینجا 1_R همان عضو خنثی در $(R,\times)$ است.

مثال 1. 1. 6 : حلقه‌های Q و Z حلقه‌های یکدار هستند.

[15] *Subgroup*
[16] *Finite*
[17] *Order*

تعریف 7.1.1 : حلقه‌ی $(R , + ,\times)$ را حلقه‌ای جابجایی[18] یا تعویض‌پذیر می‌گوییم هرگاه

$$\forall\, a,b \in R \quad ; \quad a.b = b.a\,.$$

تعریف 8.1.1 : عضو a از حلقه‌ی R را پوچتوان[19] می نامیم، اگر عدد صحیحی چون m وجود داشته باشد، بطوریکه $a^m = ۰$. اگر a در R پوچتوان باشد آنگاه $۰ < m \leq |R|$ ، و m را شاخص(اندیس پوچتوانی) a می نامیم.

تعریف 9.1.1 : عضو غیرصفر a از حلقه‌ی R را مقسوم‌علیه صفر[20] می نامیم، هرگاه عضو غیرصفر b از حلقه‌ی R را داشته باشیم، بطوریکه $ab = ba = ۰$.

اگر فقط یکی از روابط فوق برقرار باشند، مقسوم‌علیه را چپ یا راست صفر می‌گوییم. واضح است که اگر حلقه‌ی R دارای عضو پوچتوان باشد، آنگاه مقسوم علیه صفر نیز دارد.

مثال 10.1.1: در حلقه‌ی Z_6 داریم: $\bar{2}.\bar{3} = ۰$ و $\bar{4}.\bar{3} = ۰$ یعنی ۳ مقسوم علیه صفر است.

تعریف 11.1.1: حلقه‌ی جابجایی و یکدار R را حوزه صحیح[21] (قلمرو صحیح) می نامیم، هرگاه فاقد مقسوم-علیه صفر باشد.

مثال 12.1.1: حلقه‌های C, Q , Z فاقد مقسوم‌علیه صفر هستند و چون جابجایی ویکدارند، بنابراین حوزه صحیح می‌باشند.

تذکر 13.1.1: در هر حوزه صحیح R قانون حذف برقرار است. زیرا اگر $ab = ac$ و $a \neq ۰$ باشد، آنگاه $a(b - c) = ۰$، که چون R فاقد مقسوم‌علیه صفر است بایستی $b - c = ۰$ یعنی $b = c$. همچنین عکس این مطلب نیز برقرار است، زیرا اگر $a \neq ۰$ و $a.b = ۰ = ۰.a$ آنگاه $b = ۰$.

---

[18] Commutative
[19] Nilpotent
[20] Zero Divisor
[21] Integral Domain

تعریف 1. 14.1 : زیرمجموعه‌ی ناتهی $S \subseteq R$ را زیرحلقه[22] R می نامیم، هرگاه S تحت اعمال R خود یک حلقه باشد.

لم 1. 1. 15 : زیرمجموعه‌ی ناتهی $S \subseteq R$ زیرحلقه است، اگروفقط‌اگر برای هر $a, b \in S$ ، داشته باشید:

$$a - b \, , ab \; \in S.$$

مثال 1 .1. 16: مجموعه اعداد صحیح یک زیرحلقه برای مجموعه اعداد گویا است.

لم 1. 1. 17 : فصل مشترک هر تعداد از زیرحلقه‌های R یک زیرحلقه R است. به عبارت دیگر اگر $\{S_i | i \ \in I\}$ ها خانواده زیرحلقه‌های R باشند و S اشتراک آنها باشد، آنگاه S نیز زیرحلقه R است. فرض کنید C زیرمجموعه ناتهی از حلقه R باشد قرار می دهیم:

$$[\, C \,] = \cap \, S_i \qquad\qquad , \qquad S_i \leq R.$$

در اینصورت $[\, C \,]$ زیرحلقه‌ی R است زیرا فصل مشترک زیرحلقه هاست. از طرفی $C \subseteq [\, C \,]$. لذا $[\, C \,]$ کوچکترین زیرحلقه R است که شامل C می باشد. این زیرحلقه را زیرحلقه تولید شده به وسیله C می نامیم. اگر $C \subseteq R$ خود یک زیرحلقه باشد، در اینصورت $C = [\, C \,]$.

تعریف 1 .1 .18 : مشخصه‌ی حلقه‌ی[23] R ، کوچکترین عددصحیحی و مثبتی مانند n است، بطوریکه برای هر $a \in R$ داشته باشیم :

$$na = a + a + a + \ \dots \ \ a = ۰ \, .$$

اگر چنین عددی موجود نباشد مشخصه‌حلقه صفر تعریف می شود.

لم ۱. ۱. 19: مشخصه هر حوزه‌ی صحیح صفر یا عددی اول است.

اثبات : فرض کنید که مشخصه R برابر $n > ۰$ و R حوزه صحیح باشد. اگر n عددی اول نباشد می‌دانیم که

[22] *Sub Ring*
[23] *Char*

$$\circ = n\,.\,1_R = (n_1\,.\,n_2\,).\,1_R = (n_1\,.\,1_R\,).\,(n_2\,.\,1_R).$$

حال چون R حوزه صحیح است، بایستی $n_1.\,1_R\ = \circ$ یا $n_2\,.\,1_R\ = \circ$ باشد. چون $n_1\,, n_2 < n$، این مطلب تناقض با مشخصه بودن n را ایجاد می‌کند بنابراین n عددی اول است.

تعریف ۱. ۱ .20 : فرض‌کنید R و R' دوحلقه باشند، تابع $f\,:\,R\ \to\ R'$ را یک همریختی[24] می‌نامیم، هرگاه :

$$\forall\, x\,, y\ \in R\ ,\quad f(x+y) = f(x) + f(y),$$
$$f(x.\,y) = f(x).\,f(y).$$

هرگاه همریختی $f\,:\,R\ \to\ R'$ یک‌به‌یک وپوشا باشد، آنگاه f را یک یکریختی[25] می‌گوییم. دراینصورت R و R' را یکریخت می نامیم، و با نماد $R \approx R'$ نشان می‌دهیم.

هر یکریختی $f\,:\,R\ \to\ R$ را یک خودریختی[26] می‌گوییم.

مثال 1. 1. 21 : تابع

$$\varphi\ :Z\ \to Z_m\,,$$
$$\varphi(m) = m$$

یک همریختی است. زیرا

$$\overline{a+b}\ = \bar{a} + \bar{b},$$
$$\overline{a.\,b} = \bar{a}.\bar{b}.$$

[24] *Homomorphism*
[25] *Isomorphism*
[26] *Automorphism*

تعریف 1. 1. 22 : فرض کنیدکه R یک حلقه باشد. زیرحلقه I از حلقه R را ایده‌آل[27] چپ (راست) R می-نامیم، هرگاه برای هر x از I و r از R، rx عضو I باشد.(اگر xr عضو I باشد ایده‌آل مورد نظر را ایده‌آل راست می نامیم).

مثال ۱. ۱. 23: برای هر حلقه R همواره $I = \{ ۰ \}$ و $I = R$ ایده‌آل های R هستند که آنها را بدیهی[28] می نامیم.

لم ۱. ۱. 24: اگر I ایده‌آل R باشد و ۱ عضو I باشد، $I = R$ است و بالعکس.

اثبات : اگر $I = R$ چون $1 \in R$ بنابراین $1 \in I$. حال اگر $1 \in I$ ، آنگاه برای هر $r \in R$،

$r.1 \in I$ یعنی $R \subseteq I$ ، و چون همواره $I \subseteq R$ در نتیجه $R = I$.

لم ۱. ۱. 25: اگر I ایده‌آلی از حلقه R باشد و $a \in I$ وارون‌پذیر باشد ، آنگاه $I = R$.

اثبات : اگر $a \in I$ باشد، چون a در R وارون پذیر است بنابراین $a.a^{-1} = 1 \in I$. و در نتیجه طبق لم (۱. ۱. 24) ، $I = R$.

تعریف ۱. ۱. 26 : ایده‌آل I از حلقه R اصلی[29] نامیده می شود، اگروفقطاگر توسط یک عضو تولید شود. حلقه جابجایی و یکدار R را حلقه(حوزه) ایده‌آل های اصلی[30] می‌نامیم، هرگاه هر ایده‌آلش اصلی باشد. به عبارت دیگر اگر I ایده‌آل R باشد، آنگاه عضوی چون $a \in R$ وجود داشته باشد بطوریکه $I = \langle a \rangle$.

مثال ۱. ۱. 27: میدان Q یک حوزه ایده‌آل‌های اصلی است، زیرا ایده‌آل های Q ، $\{۰\}$ و خود Q هستند،که اصلی هستند.

تعریف ۱. ۱. 28: ایده‌آل $M \neq R$ از حلقه R را بیشین[31] می نامیم، هرگاه اگر J ایده‌آل دیگری از R باشد بطوریکه $M \subseteq J$ آنگاه، $M = J$ یا $J = R$.

---

[27] *Ideal*
[28] *Trivial*
[29] *Principal*
[30] *Principal Ideal Domain (PID)*

تعریف ۱. ۱. 29: حلقه‌ی جابجایی و یکدار F را میدان می‌نامیم، هرگاه هر عضو غیرصفرش وارون داشته باشد. به طورکلی مجموعه غیرتهی F تحت دوعمل $+$ و $\times$ میدان است، هرگاه :

۱) مجموعه ی $(F\ ,+)$ و مجموعه ی $(F-\{\circ\},\times)$ گروه های آبلی باشند.

۳) ضرب نسبت به جمع خاصیت توزیع پذیری داشته باشد.

مثال ۱. ۱. 30: مجموعه‌های اعدادحقیقی و اعدادگویا میدان هستند، اما مجموعه اعدادصحیح میدان نیست. همچنین Z_p یا مجموعه اعدادصحیح به هنگ عدد اول p یک میدان p عضوی می باشد.

لم ۱. ۱. 31: هر میدان یک حوزه‌صحیح است.

اثبات : اگر $a\ ,b\ \in F$ و $ab=\circ$ و $a\neq\circ$ باشد، آنگاه چون F میدان است بنابراین $a^{-1}\in F$ وجود دارد، بطوریکه

$$a^{-1}(a.b)=a^{-1}.\circ$$

در نتیجه $b=\circ$. یعنی F فاقد مقسوم علیه صفر است.

عکس لم (۱. ۱. 31) لزوما برقرار نیست، به عبارت دیگر هر حوزه‌صحیحی، لزوما یک میدان نمی‌تواند باشد.

تعریف ۱. ۱. 32: مجموعه $F'\subseteq F$ را زیرمیدان F می‌گوییم، هرگاه F' تحت اعمال F خود یک میدان باشد. میدان اعدادگویا زیرمیدانی از میدان اعداد حقیقی است.

تعریف 1.1. ۳۳ : میدان F را یک میدان اول[۳۲] می نامیم، اگربجز خودش زیرمیدان دیگری نداشته باشد.

مثال1. 1. ۳٤ : برای هر عدداول p ، Z_p میدانی اول است. زیرا اگر F زیرمیدانی از Z_p باشد، در اینصورت طبق تعریف بایستی F زیرگروهی آبلی تحت عمل جمع از Z_p باشد، یعنی

$$(F,+)\leq(Z_p,+),$$

[31] $Maximal$
[32] $Prime\ Field$

ودر نتیجه $|F| \mid |Z_p| = p$.

یعنی $|F| = p$ و در نتیجه $F = Z_p$. یعنی برای هر عدداول p ، Z_p میدانی اول است.

می توان گفت که هر زیرمجموعه از p عضو مجزای F_q با یک میدان F_p یکریخت است. بنابراین هر میدان F_q شامل یک میدان F_p است،که زیرمیدان اول F_q نامیده می‌شود.

قضیه 35.1.1 : اگر F_q میدان متناهی با q عضو باشد، آنگاه

۱) همواره q به صورت توانی از یک عدداول p است که در آن p مشخصه‌ی میدان است.

۲) میدان F_q شامل زیرمیدان F_p است.

۳) میدان F_q یک فضای برداری روی F_p از بعد m است اگروفقطاگر، $q = p^m$.

۴) برای تمامی $a \in F$، داریم $pa = 0$.

۵) میدان F_q تحت یکریختی ثابت و منحصربفرد می‌ماند.

2.1 حلقه های خارج قسمتی

تعریف ۱.۲.۱ : اگر R یک حلقه باشد و I ایده‌آل R باشد، آنگاه $\frac{R}{I}$ را بصورت زیر تعریف می‌کنیم، و آنرا حلقه‌ی خارج قسمتی[33] می نامیم.

$$\frac{R}{I} = \{ a + I \mid a \in R \},$$

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I).(b + I) = ab + I.$$

تعریف 2.2.1 : اگر $f : R \to S$ یک همریختی باشد، هسته[34] f را بصورت زیر تعریف می‌کنیم:

---

[33] *Division Ring*
[34] *Kernel*

$$Ker(f) = \{x \in R \mid f(x) = 0\}.$$

قضیه ۱ .۲. 3 (قضیه اساسی همریختی) : اگر $f : R \to S$ یک همریختی باشد، در اینصورت همریختی یک به یکی مانند $\overline{f}$ بصورت

$$\overline{f} : \frac{R}{Ker\,(f)} \to S,$$

وجود دارد بطوریکه $f = \bar{f} o \phi_I$. که در آن

$$\phi_I : R \to \frac{R}{Ker(\,f\,)}$$ و

$$\phi_I(x) = x + Ker(\,f\,).$$

اثبات : تابع $\overline{f}$ را بصورت زیر تعریف می کنیم :

$$\overline{f} : \frac{R}{Ker\,(f)} \to S,$$

$$\overline{f}\,(\,a + I\,) = f(a).$$

$\overline{f}$ خوش تعریف است. زیرا اگر $a + I = b + I$ باشد، آنگاه $a - b \in I = ker(f)$ و در نتیجه $f(a - b\,) = 0$. از آنجاییکه f همریختی است بنابراین $f(a) - f(b) = 0$، و $f(a) = f(b)$. یعنی $\overline{f}\,(\,a + I\,) = \overline{f}\,(b + I\,)$، و درنتیجه $\overline{f}$ خوش‌تعریف و یک‌به‌یک است. $\overline{f}$ همریختی است زیرا f همریختی است. همچنین

$$\bar{f} o \phi_I(x) = \bar{f}(\phi_I(x)\,) = \bar{f}(x + I\,) = f(x).$$

یعنی $\bar{f} o \phi_I = f$.

نتیجه ۱ .۲. 4 : اگر $f : R \to S$ همریختی باشد، آنگاه $f(R) \approx \frac{R}{Ker\,(f)}$.همچنین اگر f (یکریختی) باشد چون $f(R) = S$ در نتیجه $\frac{R}{Ker\,(f)} \approx S$.

مثال ۱ .۲. 5 : تابع