بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

دانشگاه پیام نور استان تهران
مرکز تهران شرق
دانشکده‌ی علوم پایه

کدهای دوری و پاد دوری روی حلقه های زنجیری متناهی

پایان نامه برای دریافت درجه کارشناسی ارشد
در رشته ریاضی محض گرایش جبر

پریناز عبادزاده فرد

اساتید راهنما:
دکتر محمد حسن بیژن زاده
دکتر ناصر زمانی

استاد مشاور:
دکتر فیصل حسنی

بهمن ماه ۱۳۹۱

بسمه تعالی

صورتجلسه دفاع از پایان‌نامه کارشناسی ارشد

نام مرکز: دانشگاه پیام نور تهران؛ مرکز تهران شرق

نام دانشجو: پریناز عبادزاده فرد

شماره دانشجویی: ۸۹۰۰۷۱۷۴۵

رشته: ریاضی محض

گرایش: جبر

عنوان پایان‌نامه: کدهای دوری و پاددوری روی حلقه های زنجیری متناهی

تاریخ دفاع: ۷ / ۱۱ / ۱۳۹۱

نمره و درجه پایان‌نامه:

ردیف	سمت	نام و نام خانوادگی	مرتبه	دانشگاه یا مؤسسه	امضا
۱	استاد راهنما	دکتر محمد حسن بیژن زاده	استاد تمام	دانشگاه پیام نور تهران	
۲	استاد راهنمای همکار	دکتر ناصر زمانی	دانشیار	دانشگاه محقق اردبیلی	
۳	استاد مشاور ۱	دکتر فیصل حسنی		دانشگاه پیام نور تهران	
٤	استاد مشاور ۲				
٥	استاد داور	دکتر داریوش کیانی	دانشیار	دانشگاه صنعتی امیر کبیر	
٦	نماینده گروه آموزشی و پژوهشی استان	دکتر فهیمه سلطانیان		دانشگاه پیام نور تهران	

گواهی اصالت، نشر و حقوق مادی و معنوی اثر

اینجانب پریناز عبادزاده فرد دانشجوی ورودی سال
۱۳۸۹ مقطع کارشناسی ارشد
رشته ریاضی محض جبر گواهی می نمایم چنان‌چه در پایان نامه خود از فکر، ایده و نوشته دیگری بهره گرفته‌ام با نقل‌قول مستقیم یا غیرمستقیم منبع و ماخذ آن را نیز در جای مناسب ذکر کرده ام .بدیهی است مسئولیت تمامی مطالبی که نقل‌قول دیگران نباشد بر عهده خویش می دانم و جوابگوی آن خواهم بود.
دانشجو تأیید می‌نماید که مطالب مندرج دراین پایان نامه نتیجه تحقیقات خودش می باشد و در صورت استفاده از نتایج دیگران مرجع آن را ذکر نموده است.

نام و نام خانوادگی دانشجو: پریناز عبادزاده فرد
تاریخ و امضاء:

اینجانب پریناز عبادزاده فرد دانشجوی ورودی سال۱۳۸۹ مقطع کارشناسی ارشد
رشته ریاضی محض جبر گواهی می‌نمایم چنانچه براساس مطالب پایان‌نامه خود اقدام به انتشار مقاله، کتاب، و .... نمایم ضمن مطلع نمودن استاد راهنما، با نظر ایشان نسبت به نشر مقاله، کتاب، و ... و به صورت مشترک و با ذکر نام استاد راهنما مبادرت نمایم.

نام و نام خانوادگی دانشجو: پریناز عبادزاده فرد
تاریخ و امضاء:

(کلیه حقوق مادی مترتب از نتایج مطالعات ، آزمایشات و نو آوری ناشی از تحقیق موضوع این پایان نامه متعلق به دانشگاه پیام نور می باشد.)

تقدیم به :

یگانه بهانه زندگیم : همسر مهربانم

به پاس تمام لحظه های همدلی و محبت بی دریغ ات که همواره تکیه گاه امن زندگیم هستی.

تقدیر و تشکر:

سپاس و ستایش معبود یگانه را که پرتو الطاف بی شمارش بر لحظه لحظه زندگیم ساطع و آشکار است. حمد و ثنا می گزارم او را که فکرت و اندیشه را در بستر روحم روان ساخت و بهره گیری از خوان گسترده دانش اساتیدم را روزی ام گردانید.

بعد از حمد و سپاس خدای منان، بر خود لازم می دانم از زحمات مادر دلسوز و پدر گرامی‌ام نهایت تشکر را داشته باشم، که دلگرمی و دعاهای خیرشان تحمل مشکلات را برایم مقدور می‌گرداند. و هیچ واژه‌ای قادر به تحسین و ستایش عظمت مادر مهربان و پدر عزیزم نیست.

امتنان و سپاس می گزارم تلاشها، زحمات و راهنمایی های ظریف، ارزشمند و بی شائبه ی اساتید فرزانه و گرانمایه ام، جناب آقای دکتر بیژن زاده و جناب آقای دکتر ناصر زمانی که با حمیت و جدیت، مرا به دقت، اندیشه، درک و تعمق وا می داشتند. امید به اینکه شایستگی شاگردی ایشان را دارا بوده باشم و دوباره توفیق افتخار شاگردی ایشان نصیب من گردد.

چکیده: ساختار کدهای دوری و پاددوری از طول n و دوگانهای آنها روی حلقه زنجیری متناهی R وقتی که مشخصهٔ میدان $\bar{R}$، عدد n را عاد نکند، بررسی می شوند. نیز بعضی حالتهایی که مشخصهٔ میدان $\bar{R}$ عدد n را عاد می کند، بررسی می شوند. مثلاً ساختار کدهای پاددوری از طول ۲^t و دوگانهای آنها روی حلقه $Z_{۲^m}$ مطالعه می شوند.

کلید واژه‌ها : حلقه های زنجیری، کدهای دوری، کدهای دوگان، کدهای پاددوری، کدهای خوددوگان.

فهرست مندرجات

فهرست جداول

مقدمه

مقاله‌ی سال ۱۹۴۸ شانون با عنوان نظریه‌ی ریاضی ارتباطات را می توان نقطه آغاز آنچه که امروزه به نظریه اطلاعات معروف است دانست. مبحث اصلی نظریه کد گذاری مطالعه روش هایی برای انتقال اطلاعات به صورت دقیق و کارآمد از محلی به محل دیگر است. چنین روش هایی می توانند کاربرد های بسیار متنوعی داشته باشند. انتقال اطلاعات مالی از طریق خطوط تلفن، ارسال تصاویر و سایر اطلاعات از فضا، دو نمونه از این کاربرد ها هستند. واسطه فیزیکی که برای انتقال اطلاعات به کار می رود کانال نامیده می شود؛ مانند خطوط تلفن، اتمسفر و یا خطوط ارتباط ماهواره ای. عوامل نامطلوبی که سبب می شوند اطلاعات ارسال شده با آنچه در طرف دیگر دریافت می شود، متفاوت باشد اختلال نام دارد، مانند خراش های روی یک دیسک فشرده، پارازیت روی خطوط رادیویی، رعد و برق و غیره. گاهی ممکن است که با تکرار اثر خطا را از بین ببریم. نظریه کد گذاری با مسئله کشف و تصحیح خطاهای به وجود آمده در انتقال که از اختلال در کانال ناشی می شوند، سر و کار دارد. ایده‌ی اصلی این است که به جز اطلاعات مورد نظر، اطلاعات اضافی خاصی نیز ارسال شود تا در صورتی که اثر اختلال (تعداد خطاها) از حد مشخصی بیشتر نباشد، بتوان اطلاعات اصلی را باز یابی کرد. به عبارتی، اطلاعات باید پیش از ارسال به کانال کد گذاری شوند.

شاخه ای از این نظریه که ابزار های جبری مانند ماتریس ها و جبر خطی روی میدان های متناهی را به کار می گیرد، به نظریه کدگذاری جبری معروف شده و به صورت یک زمینه مطالعاتی و پژوهشی مستقل در آمده است. مطالعه کدها روی حلقه های متناهی پس از انتشار مقاله کالدر بانک [۷] و دیگران که کدهای غیرخطی را به کدهای خطی روی حلقه Z_4 ارتباط می دهد، به طور فزاینده ای اهمیت پیدا می کند. پیشرفت ها در این زمینه در جهت شناسایی خواص ساختاری کدها روی خانواده گسترده ای از حلقه ها مانند حلقه های

فروبینیوس و حلقه های زنجیری ادامه پیدا می کند. این پایان نامه در این راستا نگارش شده است. چند قضیه ساختاری در مورد کدهای دوری، پاددوری و دوگان های آنها استنتاج می شوند. فرض کنیم R یک حلقه زنجیری با ایده آل ماکسیمال (a) باشد. از روش به کار رفته در منبع [۷] استفاده کرده و کدهای دوری و دوری خوددوگان از طول n روی R ارائه می دهیم، به شرطی که $(n,p)=1$، که در آن p مشخصه $\bar{R}=\frac{R}{(a)}$ می باشد. به طور کامل ساختار کدهای دوری و دوگان آنهامعین شده و شرایط لازم و کافی برای وجود کدهای خوددوگان دوری غیر بدیهی ارائه می شوند. اگر n فرد باشد، کدهای دوری و دوگان آنها نیز با تحمیل شرط اضافی به روش مشابه شناسایی می شوند. بعلاوه ساختار کدهای پاددوری از طول 2^t روی Z_{2^m} به دست خواهد آمد.

فصل ۱

تعاریف و مقدمات اولیه

در این فصل، مقدماتی در مورد حلقه ها و برخی حلقه های متناهی که در ادامه استفاده می شوند، ارائه شده است. اثبات اغلب آنها را می توان در [۱٦] پیگیری کرد.
در سراسر پایان نامه R حلقه‌ای جابجایی و یکدار است. اغلب R حلقه ای متناهی است، اگرچه همواره تاکید خواهد شد.
یادآوری می کنیم ایده آل I از حلقه R اصلی [۱] است، هرگاه $a \in R$ موجود باشد به طوری که $I =< a >$. اگر همه ایده آل های حلقه R اصلی باشد، آن را حلقه ایده آل اصلی [۲] می نامیم. حلقه R را حلقه زنجیری [۳] می نامیم هرگاه مجموعه ایده آل های آن با رابطه شمول، مرتب کلی باشد. در مورد حلقه های زنجیری قضیه زیر برقرار است.

گزاره ۱.۱. برای هر حلقه جابجایی متناهی R، شرایط زیر معادل اند:
۱) R حلقه موضعی است و ایده آل ماکسیمال M از R اصلی است.
۲) R حلقه ایده آل اصلی موضعی است.
۳) R حلقه زنجیری است.

اثبات: (۲) $\rightarrow$ (۱) فرض کنیم R حلقه موضعی و ایده آل ماکسیمال M از R توسط a تولید شود. فرض کنیم I ایده آلی از R باشد. اگر $I = (R)$ باشد چیزی برای اثبات وجود

---

[۱] principal
[۲] principal ideal ring
[۳] chain ring

ندارد.

اگر $I \subset R$ پس $I \subset M$. چون R حلقه موضعی و تنها یک ایده آل ماکسیمال دارد و نیز ایده آل ماکسیمال M از R اصلی است پس M فقط توسط یک عضو تولید می شود لذا $M =< a >$. پس عدد صحیح k وجود دارد که $I = a^k$ لذا R حلقه ایده آل اصلی موضعی است.

$(۲) \to (۳)$ فرض کنیم R حلقه ایده آل اصلی موضعی با ایده آل ماکسیمال $M =< a >$ باشد و A و B ایده آل های سره R باشند. لذا $A, B \subset M$ از این رو اعداد صحیح m و l وجود دارند که $A =< a^l >$ و $B =< a^m >$ (اعداد m و l از اندیس پوچتوانی کوچکتر هستند). بنابراین $A \subset B$ یا $B \subset A$. لذا R حلقه زنجیری است.

$(۳ \to ۱)$ فرض کنیم R حلقه زنجیری است، به وضوح R حلقه موضعی است. نشان می دهیم ایده آل ماکسیمال M از R اصلی است.

فرض کنیم ایده آل ماکسیمال M اصلی نبوده و توسط بیش از یک عضو تولید شود. فرض کنیم b و c مولد های M باشند و $b \notin cR$ ، $c \notin bR$. پس $< b > \not\subseteq < c >$ ، $< c > \not\subseteq < b >$، که با حلقه زنجیری بودن R در تناقض است. لذا فرض خلف باطل و M ایده آل اصلی است.

در این پایان نامه که با حلقهٔ زنجیری متناهی مانند R سروکار داریم، از گزاره فوق الذکر استفاده خواهد شد. اگر مانند اثبات گزاره بالا $M =< a >$، آنگاه a پوچتوان است و کوچکترین توانی از a مانند t که $a^t = ۰$، به اندیس پوچتوانی a موسوم است. در این صورت ایده آل های R به صورت

$$R =< a^۰ > \supseteq < a^۱ > \supseteq \cdots \supseteq < a^{t-۱} > \supseteq < a^t > =< ۰ >$$

هستند. قرار می دهیم $\bar{R} = \frac{R}{M}$. هomomorfism طبیعی $- : R[x] \longrightarrow \bar{R}[x]$ که $r \in R$ را به $r + M$ و x رابه x می نگارد در نظر می گیریم. در ادامه مطالبی را در مورد حلقه های زنجیری جابجایی متناهی گردآوری می کنیم. یادآوری می کنیم که عضو $f(x) \in R[x]$ را تحویل ناپذیر اساسی یا تحویل ناپذیر اساسی [۴] می نامیم اگر $\bar{f}$ در $\bar{R}[x]$ تحویل ناپذیر باشد. چند جمله ای $f(x) \in R[x]$، تحویل ناپذیر [۵] است اگر $f(x) = g(x).h(x)$ که $g(x), h(x) \in R[x]$، آنگاه یا $g(x)$ یا $h(x)$ عنصر وارون پذیر در R باشند. $f(x) \in R[x]$ منظم

[۴] basic irreducible

[۵] irreducible

[6] است اگر مقسوم علیه صفر نباشد.

گزاره ۲.۱. فرض کنیم R حلقه زنجیری متناهی با ایده آل ماکسیمال $M =< a >$ و اندیس پوچتوانی t باشد. گزاره های زیر برقرار هستند.

۱) عدد اول p و اعداد صحیح مثبت k و l که $(k \geq l)$ وجود دارند که $|R| = p^k$ و $|\bar{R}| = p^l$ و مشخصه R و $\bar{R}$ توان هایی از p اند.

۲) برای $i = ۰, ۱, \cdots, t$ داریم $| < a^i > | = |\bar{R}|^{t-i}$. به ویژه $|R| = |\bar{R}|^t$ و $k = lt$.

اثبات: از آنجا که $\bar{R}$ میدان متناهی است، پس عدد اول p و عدد صحیح مثبت l وجود دارند که $|\bar{R}| = p^l$.

حال چون $(۰ : m^{t-۱}) \supseteq m$ پس

$$\frac{m^{t-۱}}{m^t} = \frac{m^{t-۱}}{\{۰\}} = \frac{< a^{t-۱} >}{\{۰\}}$$

و لذا $m^{t-۱}$ فضای برداری یک بعدی روی $\bar{R}$ است. پس $\bar{R} \cong m^{t-۱}$ و لذا $|\bar{R}| = |m^{t-۱}|$.

مشابهاً $(۰ : \frac{m^{t-۲}}{m^{t-۱}}) \supseteq m$ و لذا $\frac{m^{t-۲}}{m^{t-۱}}$ فضای برداری یک بعدی روی $\bar{R}$ است. پس

$$|\frac{m^{t-۲}}{m^{t-۱}}| = |\frac{R}{M}| = p^l \Rightarrow |m^{t-۲}| = |m^{t-۱}|.p^l = p^l.p^l = p^{۲l}$$

با تکرار این روند $|m^{t-t}| = p^{tl}$ که $m^{t-t} = m^{(۰)} = R$ و برهان تمام می شود.

گزاره ۳.۱. فرض کنیم $f = a_۰ + a_۱x + \cdots + a_nx^n \in R[x]$. عبارت های زیر معادل اند:

۱) f منظم است.

۲) $< a_۰, a_۱, \cdots, a_n >= R$.

۳) i ای وجود دارد که $۰ \leq i \leq n$ و a_i یکه است.

۴) $\bar{f} \neq ۰$.

اثبات: فصل ۱۳ منبع ۱٦ دیده شود.

لم ۴.۱. لم هانسل. فرض کنیم f چند جمله ای روی R و $\bar{f} = g_۱ \cdots g_r$ که $g_۱$، $\cdots$، g_r چندجمله ای های دو به دو نسبت به هم اول روی $\bar{R}$ هستند. در این صورت چندجمله ای

---

[6] regular

های دو به دو نسبت به هم اول $f_۱$، $\cdots$، f_r روی R وجود دارند که $f = f_۱ f_۲ \cdots f_r$ و

$$\forall\ i = ۱, ۲, \cdots, r \qquad \bar{f_i} = g_i.$$

اثبات: فصل ۱۳ منبع [۱٦] دیده شود.

تعریف ۵.۱. میدانی مانند F، جبری بسته [۷] نامیده می شود، اگر هر چند جمله ای غیر ثابت $f(x) \in F[x]$ یک ریشه در F داشته باشد.

تعریف ٦.۱. اگر E و F میدان باشند، E یک توسیع [۸] از F گفته می شود اگر E شامل زیر میدانی ایزومرفیسم با F باشد.

تعریف ۷.۱. $\bar{k}$ بستار جبری [۹] از میدان k است اگر اولاً یک توسیع جبری از k باشد، ثانیاً جبری بسته باشد.

فرض کنیم L مجموعه همه چند جمله ای های $f \in R[x]$ باشد که $\bar{f}$ دارای صفرهای مجزا در بستار جبری $\bar{R}$ است.گزاره زیر ارتباط بین تحویل ناپذیری و تحویل ناپذیری اساسی چندجمله ای های منظم و عناصر L رانشان می دهد.

تعریف ۸.۱. چند جمله ای $f(x) \in R[x]$، تحویل ناپذیر [۱۰] نامیده می شود، اگر $f(x) = g(x).h(x)$ که $g(x), h(x) \in R[x]$، آنگاه $g(x)$ یا $h(x)$ در $R[x]$ وارون پذیر باشند.

گزاره ۹.۱. فرض کنیم f چند جمله ای منظم باشد. در این صورت

۱) اگر f تحویل ناپذیر اساسی باشد، آنگاه f تحویل ناپذیر است .

۲) اگر f تحویل ناپذیر باشد، آنگاه $\bar{f} = ug^k$، که $u \in \bar{R}$ و g تحویل ناپذیر تکین در $\bar{R}[x]$ است.

[۷] algebraically closed

[۸] extension

[۹] algebraic closure

[۱۰] irreducible

۳) اگر f عضو L باشد، آنگاه f تحویل ناپذیر است اگر و تنها اگر تحویل ناپذیر اساسی باشد.
اثبات: فصل ۱۳ منبع ۱٦ دیده شود.

تعریف ۱۰.۱. ایده آل $I \subset R$ اولیه [11] است اگر $I \neq R$ و $ab \in I$ نتیجه بدهد $a \in I$، یا عدد صحیح مثبت k وجود داشته باشد که $b^k \in I$.
چندجمله ای $f \in R[x]$ اولیه نامیده می شود اگر $< f >$ یک ایده آل اولیه در $R[x]$ باشد.

گزاره ۱۱.۱. فرض کنیم $f(x)$ چند جمله ای منظم در $R[x]$ باشد، در این صورت $f = ug_1 \cdots g_r$، به طوری که u یکه است و g_1، $\cdots$، g_r چندجمله ای های نسبت به هم اول، اولیه منظم اند. بعلاوه g_1، $\cdots$، g_r منحصر به فرد اند، یعنی اگر $f = ug_1 \cdots g_r = vh_1 \cdots h_r$ که u و v یکه و $\{g_i\}$ و $\{h_i\}$ چندجمله ای های متباین اولیه منظم باشند. آنگاه $r = s$ و برای $1 \leq i \leq n$ داریم $< g_i > = < h_i >$.
اثبات: فصل ۱۳ منبع ۱٦ دیده شود.

تعریف ۱۲.۱. فرض کنیم $f_1(x), f_2(x) \in R[x]$. $f_1(x)$ وابسته [12] به $f_2(x)$ نامیده می شود، اگر عضو وارون پذیر $r \in R$ وجود داشته باشد به طوری که $f_1(x) = rf_2(x)$.

نتیجه ۱۳.۱. چندجمله ای منظم f اولیه است اگر و تنها اگر $\bar{f}$ در $\bar{R}[x]$ اولیه باشد. معادلاً $\bar{f} = u\bar{g}^n$ که $u \in \bar{R}$ و $\bar{g}$ تحویل ناپذیر در $\bar{R}[x]$ است.

تعریف ۱۴.۱. چند جمله ای $f(x) \in R[x]$، را آزاد از مربع [13] می گوییم هرگاه چندجمله ای غیر یکال $g(x) \in R[x]$ موجود نباشد که $g^2(x)|f(x)$.

---
[11] primary
[12] associate
[13] square free

گزاره ۱.۱۵. اگر $f(x)$ یک چند جمله ای تکین روی R و $\bar{f}$ آزاد از مربع باشد، آنگاه $f(x)$ به صورت حاصلضرب چندجمله ای های تکین دو به دو نسبت به هم اول، که تحویل ناپذیر پایه ای هستند، تجزیه می شود.

اثبات: فرض کنیم $f(x)$ یک چند جمله ای تکین روی R و $\bar{f}$ آزاد از مربع باشد. پس $\bar{f}$ ریشه مکرر ندارد. لذا داریم:

$$\bar{f} = g_1^1(x).g_2^1(x).\cdots.g_r^1(x), \quad g_i(x) \in \bar{R}[x]$$

و $f = f_1.\cdots.f_r$ که از قضیه ۱.۹ و لم هانسل (قضیه ۱.۴) نتیجه می شود که

$$\bar{f}_1 = g_1, \cdots, \bar{f}_r = g_r$$

پس f به ضرب چندجمله ای های تکین، دو به دو نسبت به هم اول تحویل ناپذیر پایه ای تجزیه می شود. f_i ها تحویل ناپذیر پایه ای اند، چون $\bar{f}_i$ ها یعنی g_i ها تحویل ناپذیر هستند و برهان تمام است.

الگوریتم اقلیدسی برای حلقه چندجمله ای ها روی حلقهٔ متناهی موضعی به شرح زیر است.

گزاره ۱.۱۶. فرض کنیم f, g چند جمله ای های مخالف صفر در $R[x]$ باشند، اگر g منظم باشد، آنگاه چندجمله ای های $q, r \in R[x]$ وجود دارند به طوری که

$$\deg(r) \leq \deg(g) \quad , \quad f = gq + r.$$

اثبات: فصل ۱۳ منبع ۱۶ دیده شود.

نظریه کدگذاری کلاسیک در محیط فضاهای برداری روی میدان های متناهی شکل گرفته است. برای به دست آوردن اطلاعات اولیه در این زمینه منابع [۳] ، [۱۳] ، [۱۵] و [۲۱] پیشنهاد می شوند. با تعدیل طبیعی مطالب، کدها، روی حلقه های متناهی ساخته می شوند. فرض کنیم R حلقه ای متناهی و n عدد طبیعی باشد. R^n را به عنوان $R-$ مدول در نظر میگیریم.

تعریف ۱.۱۷. زیرمجموعه $C \subset R^n$ را کد خطی [۱۴] به طول n روی R می نامیم، هرگاه C یک R —زیر مدول از R^n باشد. کد خطی $C \subset R^n$، کد دوری [۱۵] نامیده می شود، اگر به ازای هر کد واژه $x = (x_0, x_1, \cdots, x_{n-2}, x_{n-1}) \in C$، n—تایی $(x_{n-1}, x_0, \cdots, x_{n-2})$ نیز در C باشد. n—تایی $c = (c_0, c_1, \cdots, c_{n-2}, c_{n-1}) \in R^n$ با چند جمله ای $\pi(c) = c_0 + c_1 x + +c_{n-1}x^{n-1}$ در $\frac{R[x]}{<x^{n-1}>}$ که نمایش [۱۶] چندجمله ای C نامیده می شود، نظیر می شود.

قضیه ۱.۱۸. کد C به طول n روی R دوری است، اگر و تنها اگر $\pi(C) = \{\pi(c) | c \in C\}$ ایده آل ای از $\frac{R[x]}{<x^{n-1}>}$ باشد.

اثبات: $(\Leftarrow)$ فرض کنیم πC ایده آل ای از $\frac{R[x]}{<x^{n-1}>}$ و $(a_0, a_1, \cdots, a_{n-1}) \in C$.

$$\begin{aligned} & x(a_0 + a_1 x + \cdots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}) \\ &= a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}\underbrace{x^n}_{=1} \\ &= a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} \in \pi(C). \end{aligned}$$

و در نتیجه $(a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$. یعنی C دوری است.

$(\Rightarrow)$ فرض کنیم C کد دوری باشد و $(a_0, a_1, \cdots, a_{n-1}) \in C$. از این نتیجه می شود $(a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$، به این معنی است که به ازای هر $a(x) \in C$، $xa(x) \in C$. از این مطلب و خطی بودن C نتیجه می شود که به ازای هر $b(x) \in \frac{R[x]}{<x^{n-1}>}$ ، $b(x)a(x) \in C$ و لذا C ایده آل ای از $\frac{R[x]}{<x^{n-1}>}$ است.

تعریف ۱.۱۹ . اگر $x = (x_0, x_1, \cdots, x_{n-1})$ و $y = (y_0, y_1, \cdots, y_{n-1})$ در R^n باشند، ضرب اسکالر [۱۷] آنها به صورت $x.y = (x_0 y_0, x_1 y_1, \cdots, x_{n-1}y_{n-1})$ است. دو واژه x و y، متعامد [۱۸] نامیده می شوند، اگر $x.y = 0$. برای کد خطی C روی R، دوگان [۱۹] C، که با $C^\perp$ نشان

[۱۴] linear code
[۱۵] cyclic code
[۱۶] representation
[۱۷] scalar product
[۱۸] orthogonal
[۱۹] dual code

داده می شود، مجموعه همه واژه هایی از R است که به همه کدواژه های C عمود باشند، یعنی:

$$C^{\perp} = \{x \in R^n | x.y = 0, \quad \forall\ y \in C\}$$

کد C خود—دوگان [20] نامیده می شود هرگاه $C = C^{\perp}$.
قضیه زیر در مورد تعداد عناصر کدهای خطی روی Z_{p^m} در [8] ثابت شده است.

مثال ۲۰.۱. برای حلقه زنجیری متناهی R، با ایده آل ماکسیمال $<a>$ و مشخصه پوچتوانی زوج مانند t، کد $< a^{\frac{t}{2}} >$ خود—دوگان است که کد خود—دوگان بدیهی [21] نامیده می شود.
اثبات: در نظر میگیریم $C =< a^{\frac{t}{2}} >$، نشان می دهیم $C = C^{\perp}$. به ازای $ra^{\frac{t}{2}} \in C$ و به ازای هر $sa^{\frac{t}{2}} \in C^{\perp}$ داریم

$$ra^{\frac{t}{2}}.sa^{\frac{t}{2}} = rsa^{\frac{t}{2}} = 0 \Longrightarrow ra^{\frac{t}{2}} \in C^{\perp} \Longrightarrow C \subseteq C^{\perp}$$

حال از یک طرف داریم

$$|C| = | < a^{\frac{t}{2}} > | = |\bar{R}|^{\frac{t}{2}} \Longrightarrow |C|^2 = |\bar{R}|^t = |R| \Longrightarrow |C|.|C| = |R|$$

از طرف دیگر بنا بر فرمول حاصله در قسمت دوم منبع [8]، داریم $|C|.|C^{\perp}| = p^{an}$. پس $|C|.|C^{\perp}| = p^a$ و از قضیه ۲.۱ p^a برابر $|R|$ می شود، پس $|C|.|C^{\perp}| = |R|$. لذا $|C| = |C^{\perp}|$. و بنابراین $C = C^{\perp}$.

قضیه ۲۱.۱. تعداد کدواژه ها در کد خطی C به طول n، روی Z_{p^m}، p^k است که k عددی در $\{0, 1, \cdots, mn\}$ است. بعلاوه کد دوگان $C^{\perp}$، دارای p^l کدواژه است که $k + l = mn$.
با تعدیل اثبات قضیه بالا، می توان قضیه زیر را نیز اثبات کرد.

قضیه ۲۲.۱. فرض کنیم R حلقه متناهی از مرتبه p^{α} باشد. تعداد کدواژه ها در کد خطی C به طول n، روی R، p^k است که k عددی در $\{0, 1, \cdots, \alpha n\}$ است. بعلاوه کد دوگان $C^{\perp}$، p^l

[20] self-dual
[21] trivial self-dual

کدواژه دارد که $k+l=\alpha n$.

قضیه ۲۳.۱. فرض کنیم R حلقه جابجایی متناهی و

$$a(x)=a_۰+a_۱x+\cdots+a_{n-۱}x^{n-۱}\in R[x]$$

$$b(x)=b_۰+b_۱x+\cdots+b_{n-۱}x^{n-۱}\in R[x]$$

در این صورت $a(x)b(x)=۰$ در $\frac{R[x]}{<x^n-۱>}$ اگر و تنها اگر $(a_۰,a_۱,\cdots,a_{n-۱})$ بر $(b_{n-۱},b_{n-۲},\cdots,b_۰)$ و همه انتقال های دوری آن عمود باشد.

اثبات: فرض کنیم η انتقال دوری کدواژه های به طول n باشد. یعنی برای هر $(x_۰,x_۱,\cdots,x_{n-۱})\in R^n$ داشته باشیم

$$\eta(x_۰,x_۱,\cdots,x_{n-۱})=(x_{n-۱},x_۰,x_۱,\cdots,x_{n-۲})$$

بنابراین $\eta^i(b_{n-۱},b_{n-۲},\cdots,b_۰)$، به ازای $i=۱,۲,\cdots,۲n$، تمام انتقال های دوری $(b_{n-۱},b_{n-۲},\cdots,b_۰)$ هستند. فرض کنیم

$$c(x)=c_۰+c_۱x+\cdots+c_{n-۱}x^{n-۱}=a(x)b(x)\in\frac{R[x]}{<x^n-۱>}.$$

پس برای هر $k=۰,۱,۲,\cdots,n-۱$ داریم

$$c_k=\sum_{\substack{i+j=k\ \ or\ \ i+j=n+k\\ ۰\leq i\leq n-۱\\ ۰\leq j\leq n-۱}} a_ib_j$$

$$=(a_۰,a_۱,\cdots,a_k,a_{k+۱},\cdots,a_{n-۱})(b_k,b_{k-۱},\cdots,b_۰,-b_{n-۱},\cdots,b_{k+۱})$$

$$=(a_۰,a_۱,\cdots,a_{n-۱})\eta^{k+۱}(b_{n-۱},b_{n-۲},\cdots,b_{k+۱},b_k,b_{k-۱},\cdots,b_۰).$$

بنابراین $c(x)=۰$ است اگر و تنها اگر برای هر $k=۰,۱,۲,\cdots,n-۱$، $c_k=۰$، اگر و تنها اگر $(a_۰,a_۱,\cdots,a_{n-۱})$ بر $(b_{n-۱},b_{n-۲},\cdots,b_۰)$ و تمام انتقال های دوری آن عمود باشد.

در فصل ۲، در مورد جزئیات بیشتر کدهای خود—دوگان دوری غیر بدیهی، روی حلقه های زنجیری متناهی بحث خواهیم کرد.