دسترسی در سایتِ http://jnrm.srbiau.ac.ir
سال دهم، شماره پنجاه و یکم، آذر و دی ۱۴۰۳
شماره شاپا: ۲۵۸۸-۵۸۸X

دانشگاه آزاد اسلامی، واحد علوم و تحقیقات

پژوهش‌های نوین در ریاضی

کدهای دوری اریب مضاعف روی حلقه‌ی $\mathbb{F}_q + u\mathbb{F}_q$

فاطمه بختیاری[۱]، رقیه محمدی حصاری[۲]، رشید رضایی[۳*]، کریم سامعی[۴]

[(۱و۲و۳)] گروه ریاضی، دانشکده علوم ریاضی و آمار، دانشگاه ملایر، ملایر، ایران
[(۴)] گروه ریاضی، دانشکده علوم پایه، دانشگاه بوعلی سینا، همدان، ایران

تاریخ ارسال مقاله: ۱۴۰۰/۰۹/۱۲ **تاریخ پذیرش مقاله:** ۱۴۰۲/۰۴/۰۴

چکیده

در این مقاله، ساختار جبری کدهای دوری اریب مضاعف روی حلقه‌ی زنجیری $\mathbb{F}_q + u\mathbb{F}_q$ را مطالعه و چند جمله‌ای‌های مولد این رده از کدها را مشخص می‌کنیم. همچنین نشان می‌دهیم این کدها به شانزده دسته مجزا تقسیم می‌شوند. در ادامه کدهای دوری اریب مضاعف جدایی‌پذیر روی $\mathbb{F}_q + u\mathbb{F}_q$ را معرفی کرده، مجموعه‌ی مولد مینیمال و دوگان آنها را محاسبه می‌کنیم. در پایان، مثال‌هایی از کدهای دوری اریب مضاعف جدایی‌پذیر را ارائه می‌دهیم.

واژه‌های کلیدی: حلقه‌ی زنجیری، کد دوری اریب مضاعف، کد جدایی‌پذیر، مجموعه مولد مینیمال

[*] عهده‌دار مکاتبات:
Email: ras_rezaei@yahoo.com

۱- مقدمه

کدهای خطی، خانواده خاصی از کدها با ساختار جبری هستند که کاربردهای زیادی دارند. کدهای دوری رده‌ی مهمی از کدهای خطی هستند و چون آنها به صورت ایده‌آل‌هایی در حلقه‌های خارج قسمتی خاص توصیف می‌شوند ساختار جبری قوی‌ای دارند و به این ترتیب است که می‌توان نظریه کدگذاری را با جبر آمیخت. کدهای دوری ابتدا به وسیله‌ی پرنگ [۱۵] در سال ۱۹۵۷ مطالعه شدند سپس نظریه‌پردازان کدگذاری جبری یک فرآیند مطالعه سریع‌تری را از کدهای دوری برای هر دو تصحیح خطای تصادفی و تصحیح خطای پیوسته ایجاد کردند. بورخز و همکارانش در [۵]، ساختار جبری کدهای دوری $\mathbb{Z}_۲$- مضاعف به‌عنوان $\mathbb{Z}_۲[x]$- زیرمدول‌هایی از $R_{r,s}=\frac{\mathbb{Z}_۲[x]}{\langle x^r-۱\rangle}\times\frac{\mathbb{Z}_۲[x]}{\langle x^s-۱\rangle}$ را بررسی کردند. همچنین چندجمله‌ای‌های مولد این دسته از کدها و دوگان آنها را مشخص کردند. در [۱۰]، گائو و همکارانش کدهای دوری مضاعف روی $\mathbb{Z}_۴$ را به‌دست آوردند. در [۳]، ساختار جبری کدهای دوری $\mathbb{Z}_۲\mathbb{Z}_۴$- جمعی بررسی و دوگان هر یک از این کدها محاسبه شده است. علاوه بر این، برخی کدهای خطی دودویی بهینه از این خانواده از کدها ساخته شده‌اند. در [۴]، به معرفی کدهای $\mathbb{Z}_۲\mathbb{Z}_۲[u]$- جمعی پرداخته شده است. کدهای $SR-$ جمعی برای $R-$جبر، S در [۱۳] بررسی شده‌اند و ساختار جبری کدهای دوری $SR-$ جمعی مشخص شده است. بورخز و همکارانش در [۶]، ساختار کدهای خطی و دوری روی حاصل‌ضرب حلقه‌های زنجیری متناهی $\mathcal{R}_۱$ و $\mathcal{R}_۲$ را بررسی کردند.

در سال‌های اخیر، تحقیقات زیادی روی کدها با طول‌های مختلف روی حلقه‌ی $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ صورت گرفته است و این نشان می‌دهد که کدها روی این حلقه کاربردهای عملی بسیاری دارند و برای مطالعه از اهمیت بالایی برخوردارند. دینه تمام کدهای پایا دوری از طول p^s روی $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ را در [۹] مشخص کرد. اخیرا مقالات زیادی در زمینه‌ی کدگذاری وجود دارند که از حلقه‌ی چندجمله‌ای اریب استفاده کرده‌اند. انگیزه اصلی برای مطالعه‌ی کدها در این زمینه این است که چندجمله‌هایی که در این حلقه به معرض نمایش گذاشته می‌شوند از خواص بیشتری برخوردارند و بنابراین تعداد بیشتری ایده‌آل در حلقه‌ی چندجمله‌های اریب وجود دارد. کدهای دوری دارای تعمیم‌های زیادی هستند، یکی از مهم‌ترین آنها کدهای دوری اریب می‌باشند که متناظر با ایده‌آل‌های حلقه‌ی چندجمله‌ای اریب هستند.

بوچر و همکارانش در [۷] برای اولین بار کدهای دوری اریب با استفاده از حلقه‌ی چندجمله‌های اریب با یک خودریختی θ روی یک میدان متناهی با q عضو را تعریف کردند. ساختار جبری و خواص اساسی کدهای پایا دوری اریب روی حلقه‌های زنجیری متناهی و دوگان اقلیدسی و هرمیتی آنها در [۱۲] مطالعه شده است. محمدی حصاری و همکارانش در [۱۱] کدهای دوری اریب خودوگان از طول p^s روی $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ را بررسی کرده‌اند. در [۲] کدهای دوری اریب روی حلقه‌ی $\mathbb{F}_۲+v\mathbb{F}_۲$ که در آن $v^۲=v$ مورد مطالعه قرار گرفته است.

در این مقاله ساختار جبری کدهای دوری اریب مضاعف روی حلقه‌ی $\mathbb{F}_q+u\mathbb{F}_q$ را بررسی می‌کنیم. بخش دوم به تعاریف و مفاهیم مقدماتی مورد نیاز در این مقاله اختصاص دارد. بخش سوم شامل سه بخش زیر است، در زیر بخش اول، کدهای دوری اریب مضاعف دسته‌بندی می‌شوند. در زیربخش دوم، مجموعه‌ی مولد مینیمال و دوگان کدهای دوری اریب مضاعف جدایی‌پذیر بدست می‌آیند و در زیربخش پایانی، مثال‌هایی از این رده از کدها ارائه می‌شود.

۲- تعارف و مقدمات

در این بخش به ارائه‌ی برخی قضایا و تعاریفی که در این مقاله از آنها استفاده شده است می‌پردازیم.

تعریف ۱.۲. ایده‌آل I از حلقه‌ی یکدار R ایده‌آل چپ اصلی نامیده می‌شود، هرگاه هر عنصر $a\in I$ چنان موجود باشد که

$I = Ra = \{ra : r \in R\}$.
حلقه‌ی یکدار R را حلقه‌ی ایده‌آل اصلی چپ گویند، هرگاه هر ایده‌آل چپ آن اصلی باشد.

تعریف ۲.۲. حلقه‌ی تعویض‌پذیر R موضعی نامیده می‌شود، هرگاه فقط یک ایده‌آل ماکسیمال داشته باشد.

تعریف ۳.۲. حلقه‌ی R را زنجیری گویند، هرگاه ایده‌آل‌های آن با رابطه شمول کلا مرتب شده باشند. در واقع اگر γ مولد ایده‌آل ماکسیمال R باشد، آنگاه

$$R = \langle 1\rangle \supsetneq \langle\gamma\rangle \supsetneq \dots \supsetneq \langle \gamma^{e-1}\rangle \supsetneq \langle\gamma^{e}\rangle = \langle 0\rangle .$$

عدد صحیح e را درجه پوچی R می‌گویند.

تعریف ۴.۲. فرض کنیم R حلقه‌ی تعویض‌پذیر متناهی و σ یک خودریختی روی R باشد. در این‌صورت عمل جمع روی مجموعه‌ی

$$R[x,\sigma] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n : a_i \in R, n \in \mathbb{N}_0\},$$

را همان عمل جمع معمولی چندجمله‌ای‌ها در نظر گرفته و عمل ضرب را به‌گونه‌ای تعریف می‌کنیم که به ازای هر $a \in R$ داشته باشیم $x\cdot a = \sigma(a)x$. توسیع این عمل به کل $R[x,\sigma]$ آن را به یک حلقه‌ی یکدار تبدیل می‌کند که به آن حلقه‌ی چندجمله‌ای‌های اریب روی R و به هر عضو از این حلقه یک چندجمله‌ای اریب گفته می‌شود. این حلقه در حالت کلی تعویض‌پذیر نیست مگر آنکه σ خودریختی همانی باشد.

گزاره ۵.۲. [۱۲] فرض کنید n یک عدد طبیعی، R حلقه‌ی تعویض‌پذیر متناهی، σ یک خودریختی روی R و λ عنصری وارون‌پذیر در R باشد. در این صورت گزاره‌های زیر هم‌ارزند:

(۱) $x^n - \lambda$ عنصری مرکزی در $R[x;\sigma]$ است.

(۲) $\langle x^n - \lambda \rangle$ یک ایده‌آل دو طرفه است.

(۳) n مضربی از مرتبه σ و λ تحت σ پایا است.

تعریف ۶.۲. کد C به طول n روی حلقه‌ی تعویض‌پذیر R، یک زیرمجموعه‌ی ناتهی از R^n است. اگر C زیرمدولی از R^n باشد، آنگاه کد C را یک کد خطی می‌گویند.

تعریف ۷.۲. فرض کنیم σ یک خودریختی روی حلقه‌ی تعویض‌پذیر R باشد، در این صورت کد C روی R را σ-دوری اریب گویند، هرگاه تحت نگاشت ρ_σ که به صورت زیر تعریف می‌شود، بسته باشد.

$$\rho_\sigma : R^n \to R^n,$$
$$\rho_\sigma((a_0,a_1,\dots,a_{n-1})) = (\sigma(a_{n-1}),\sigma(a_0),\dots,\sigma(a_{n-2})).$$

اگر σ خودریختی همانی باشد، آنگاه C را یک کد دوری گویند.

حلقه‌ی $\mathbb{F}_q+u\mathbb{F}_q$ یک حلقه‌ی زنجیری متناهی با درجه پوچی ۲ است که در آن q توانی از یک عدد اول و $u^2=0$ است. همچنین $u\mathbb{F}_q$ تنها ایده‌آل ماکسیمال آن است.

لم ۸.۲. [۱۲] فرض کنیم $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ و $\eta \in \mathbb{F}_q^* = \mathbb{F}_q - \{0\}$. نگاشت

$$\Theta_{\theta,\eta} : \mathbb{F}_q+u\mathbb{F}_q \to \mathbb{F}_q+u\mathbb{F}_q$$

با ضابطه $\Theta_{\theta,\eta}(a+ub) = \theta(a)+u\eta\theta(b)$ را در نظر می‌گیریم. در این صورت

$$\mathrm{Aut}(\mathbb{F}_q+u\mathbb{F}_q) = \{\Theta_{\theta,\eta} : \theta \in \mathrm{Aut}(\mathbb{F}_q), \eta \in \mathbb{F}_q^*\}.$$

طبق لم فوق، هر خودریختی روی حلقه‌ی $\mathbb{F}_q+u\mathbb{F}_q$ به شکل $\Theta_{\theta,\eta}$ خواهد بود. در این مقاله قرارداد می‌کنیم $\eta=1$ و $\Theta_{\theta,1}$ را با نماد Θ نشان می‌دهیم. بعد از این اگر ابهامی پیش نیاید، به جای عبارت Θ–دوری اریب از عبارت دوری اریب استفاده می‌کنیم.

لم ۹.۲. [۱۴] فرض کنیم f و g چندجمله‌ای‌های اریب روی میدان متناهی $\mathbb{F}_q$ باشند و $f \neq 0$. در این صورت چندجمله‌ای‌های q و r در $\mathbb{F}_q[x;\theta]$ وجود دارند به طوری‌که $g = qf + r$ که در آن $r = 0$ یا $\deg(r) < \deg(f)$. در واقع، حلقه‌ی $\mathbb{F}_q[x;\theta]$ یک حوزه ایده‌آل اصلی است.

گزاره ۱۰.۲. [۱۲] فرض کنیم $f(x)$ و $g(x)$ چندجمله‌ای‌هایی در $\mathbb{F}_q[x;\theta]$ باشند به طوری‌که $f(x)g(x)$ یک چندجمله‌ای اریب مرکزی و تکین است. در این صورت $f(x)g(x) = g(x)f(x)$.

فرض کنیم $f(x)$ و $g(x)$ چندجمله‌ای‌های اریب روی $\mathbb{F}_q$ باشند. گوییم $f(x)$ یک مقسوم علیه راست (چپ) از $g(x)$ است و با نماد $f(x)|_r g(x)$ $(f(x)|_l g(x))$نشان می‌دهیم، هرگاه چندجمله‌ای اریب $h(x)$ وجود داشته باشد به طوری‌که $g(x)=h(x)f(x)$ $(g(x)=f(x)h(x))$.

تعریف ۱۱.۲. فرض کنید $f(x)$ و $g(x)$ چندجمله‌ای‌های اریب در $\mathbb{F}_q[x;\theta]$ باشند. بزرگترین مقسوم علیه چپ مشترک $f(x)$ و $g(x)$ در $\mathbb{F}_q[x;\theta]$ چندجمله‌ای تکین $d_l(x)$ است به طوری که $d_l(x)|_l f(x)$ و $d_l(x)|_l g(x)$. به‌علاوه، برای هر $j(x)$ در $\mathbb{F}_q[x;\theta]$ اگر $j(x)|_l f(x)$ و $j(x)|_l g(x)$، آنگاه $j(x)|_l d_r(x)$. چندجمله‌ای $d_l(x)$ را با نماد $\mathrm{gcld}(f(x),g(x))$ نشان می‌دهند.

فرض کنیم α و β اعداد صحیح نامنفی باشند به طوری که $n=\alpha+\beta$، در این مقاله نمادگذاری‌های زیر را به کار می‌بریم:

(۱) $R_2=\mathbb{F}_q+u\mathbb{F}_q$.

(۲) $m=\mathrm{lcm}(\alpha,\beta)$ و $k\in\{\alpha,\beta,m,n\}$ که در آن $\mathrm{lcm}(\alpha,\beta)$ کوچکترین مضرب مشترک α,β است.

(۳) $\mathcal{R}_{1,k}=\dfrac{\mathbb{F}_q[x;\theta]}{\langle x^k-1\rangle}$.

(۴) $\mathcal{R}_k=\dfrac{R_2[x;\Theta]}{\langle x^k-1\rangle}$.

(۵)

$$\mathcal{R}_{\alpha,\beta}=\mathcal{R}_\alpha\times\mathcal{R}_\beta=\{(f(x),g(x)):f(x)\in\mathcal{R}_\alpha, g(x)\in\mathcal{R}_\beta\}$$

همچنین فرض کنیم $o(\Theta)=o(\theta)|\gcd(\alpha,\beta)$ که در آن $o(\Theta)$ مرتبه خودریختی Θ است. چون x^k-1 عنصر مرکزی و تکین $\mathbb{F}_q[x;\theta]$ است، بنا به گزاره ۱۰.۲، مقسوم‌علیه‌های راست این عنصر دوطرفه‌اند. از طرفی حلقه‌ی چندجمله‌ای‌های اریب $\mathbb{F}_q[x;\theta]$ حوزه تجزیه یکتا نیست. در واقع ممکن است تجزیه‌های مختلفی برای یک چندجمله‌ای وجود داشته باشد. قرار می‌دهیم

$$\mathcal{F}_k=\{a(x)\in\mathbb{F}_q[x;\theta]: x^k-1 \text{ یک عامل تکین از } a(x)\}.$$

ملاحظه ۱۲.۲. [۱۲] حلقه‌ی چندجمله‌ای اریب $R_2[x;\Theta]$ نه اقلیدسی چپ و نه اقلیدسی راست است. با این حال الگوریتم تقسیم راست(چپ) برای برخی عناصر آن تعریف می‌شود. فرض کنیم $f(x)=a_0+a_1x+\cdots+a_rx^r$ و $g(x)=b_0+b_1x+\cdots+b_sx^s$ که b_s در R_2 وارون‌پذیر است. در این صورت عناصر $q(x)$ و $r(x)$ در $R_2[x;\Theta]$ وجود دارند به طوری‌که $f(x)=g(x)q(x)+r(x)$ $(f(x)=q(x)g(x)+r(x))$ که در آن $r(x)=0$ یا $\deg(r(x))<\deg(g(x))$.

گزاره ۱۳.۲. [۱] حلقه‌ی $\mathcal{R}_{1,k}$ حلقه‌ی ایده‌آل اصلی چپ است و ساختار ایده‌آل‌های چپ آن به صورت $\mathcal{R}_{1,k}(a(x))$ است که در آن $a(x)$ یک عامل تکین x^k-1 است.

تعریف ۱۴.۲. فرض کنیم C یک کد دوری اریب از طول $n=\alpha+\beta$ روی R_2 باشد. در این صورت C را یک کد دوری اریب R_2-مضاعف از طول (α,β) گویند، اگر

$$(\hat{c}_0,\hat{c}_1,\dots,\hat{c}_{\alpha-2},\hat{c}_{\alpha-1}|c_0,c_1,\dots,c_{\beta-2},c_{\beta-1})\in C,$$

آنگاه

$$(\Theta(\hat{c}_{\alpha-1}),\Theta(\hat{c}_0),\Theta(\hat{c}_1),\dots,\Theta(\hat{c}_{\alpha-2})|\Theta(c_{\beta-1}),\Theta(c_0),\Theta(c_1),\dots,\Theta(c_{\beta-2}))\in C.$$

فرض کنیم $\mathcal{R}_{\alpha,\beta}=\dfrac{R_2[x;\Theta]}{\langle x^\alpha-1\rangle}\times\dfrac{R_2[x;\Theta]}{\langle x^\beta-1\rangle}$.

نگاشت دوسویی از $R_2^\alpha\times R_2^\beta$ به $\mathcal{R}_{\alpha,\beta}$ وجود دارد به‌طوری که

$$(\hat{c}_0,\dots,\hat{c}_{\alpha-1}|c_0,\dots,c_{\beta-1})\mapsto(\hat{c}_0+\cdots+\hat{c}_{\alpha-1}x^{\alpha-1}|c_0+\cdots+c_{\beta-1}x^{\beta-1})=(\hat{c}(x)|c(x)).$$

تعریف ۱۵.۲. فرض کنیم $(a|b)\in R_2^\alpha\times R_2^\beta$ و $v\in R_2$. نگاشت "." را به صورت زیر تعریف می‌کنیم:

$$\cdot: R_2\times(R_2^\alpha\times R_2^\beta)\to R_2^\alpha\times R_2^\beta,$$
$$v\cdot(a|b)=(va|vb).$$

با توسیع این نگاشت، $\mathcal{R}_{\alpha,\beta}$ یک $R_2[x;\Theta]-$مدول چپ خواهد بود. بنابراین، کد دوری اریب R_2-مضاعف از

طول (α,β) به عنوان $R_2[x;\Theta]$–زیرمدول چپ از $\mathcal{R}_{\alpha,\beta}$ در نظر گرفته می‌شود.

لم ۱۶.۲. [۸] فرض کنید نگاشت ψ به صورت زیر تعریف شود:

$$\psi: R_2[x;\Theta]\to R_2[x;\Theta],$$
$$\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n}\Theta(a_i)x^i,$$

که در آن $a_i\in R_2$. در این صورت ψ یک همریختی حلقه‌ای است.

تعریف ۱۷.۲. فرض کنید $f(x)=a_0+a_1x+\cdots+a_\ell x^\ell$ عنصری در $R_2[x;\Theta]$ باشد که در آن $a_\ell\neq 0$. در این صورت $f^*(x)=a_\ell+\Theta(a_{\ell-1})x+\cdots+\Theta^\ell(a_0)x^\ell$ چندجمله‌ای متقابل $f(x)$ نامیده می‌شود. به طور معادل، $f^*(x)$ دارای نمایشی به صورت $f^*(x)=\sum_{i=0}^{\ell}\Theta^i(a_{\ell-i})x^i$ است.

لم ۱۸.۲. [۱۱] فرض کنید $f(x)$ و $g(x)$ چندجمله‌هایی در $R_2[x;\Theta]$ باشند. در این صورت

(۱) اگر $\deg(f)\geq\deg(g)$، آنگاه $(f(x)+g(x))^*=f^*(x)+x^{\deg f-\deg g}g^*(x)$.

(۲) $(fg)^*=\psi^{\deg f}(g^*)f^*$.

(۳) $(f^*)^*=\psi^n(f)$ که در آن $\deg f=n$.

فرض کنیم

$$x=(x_0,x_1,\dots,x_{\alpha-2},x_{\alpha-1}\mid \hat{x}_0,\hat{x}_1,\dots,\hat{x}_{\beta-2},\hat{x}_{\beta-1}),$$

و

$$y=(y_0,y_1,\dots,y_{\alpha-2},y_{\alpha-1}\mid \hat{y}_0,\hat{y}_1,\dots,\hat{y}_{\beta-2},\hat{y}_{\beta-1}),$$

عناصری در $R_2^\alpha\times R_2^\beta$ باشند. ضرب داخلی اقلیدسی بین x و y به صورت زیر تعریف می‌شود:

$$x\cdot y=\sum_{i=0}^{\alpha-1}x_iy_i+\sum_{i=0}^{\beta-1}\hat{x}_i\hat{y}_i.$$

دوگان کد C به صورت زیر تعریف می‌شود:

$$C^\perp=\{x\in R_2^\alpha\times R_2^\beta : x\cdot y=0,\forall y\in C\}.$$

اگر $C\subseteq C^\perp$، آنگاه C را خودمتعامد و اگر $C=C^\perp$، آنگاه C را خوددوگان می‌نامند.

تعریف ۱۹.۲. فرض کنیم C کد دوری اریب مضاعف روی R_2 از طول α,β باشد. با حذف β مختصات آخر، کد سوراخ شده C_α و با حذف α مختصات اول کد سوراخ شده C_β به‌دست می‌آید. اگر بتوان C را به صورت حاصل‌ضرب مستقیم C_α و C_β یعنی $C=C_\alpha\times C_\beta$ نوشت، آنگاه کد C را جدایی‌پذیر گویند.

۳- نتایج اصلی

در این بخش، کدهای دوری اریب R_2–مضاعف از طول α,β را بررسی می‌کنیم. در ادامه مجموعه‌ی مولد مینیمال و دوگان کدهای دوری اریب R_2–مضاعف جدایی‌پذیر از طول α,β را محاسبه می‌کنیم و در پایان مثال‌های از این دسته از کدها را ارائه می‌دهیم.

۱.۳ کدهای دوری اریب R_2–مضاعف از طول α,β

$R_2=\mathbb{F}_q+u\mathbb{F}_q$ یک حلقه‌ی زنجیری با درجه پوچی ۲ و $u\mathbb{F}_q$ تنها ایده‌آل ماکسیمال آن است. کدهای دوری اریب از طول k روی R_2 ایده‌آل‌های چپ $\mathcal{R}_k=\dfrac{R_2[x;\Theta]}{\langle x^k-1\rangle}$ هستند.

همریختی طبیعی $\mu:R_2\to\mathbb{F}_q$ با ضابطه $\mu(a_0+ub_0)=a_0$ را به‌صورت زیر توسیع می‌دهیم:

$$\mu:R_2[x;\Theta]\to\mathbb{F}_q[x;\theta],$$
$$\sum_{i=0}^{v}(a_i+ub_i)x^i\mapsto\sum_{i=0}^{v}a_ix^i.$$

همچنین این همریختی را می‌توان به $\mu:\mathcal{R}_k\to\mathcal{R}_{1,k}$ توسیع داد.

فرض کنیم C یک کد دوری اریب از طول k روی R_2 باشد. در این صورت کد کاهش یافته از C را به صورت زیر تعریف می‌کنیم:

$$\mathrm{Res}(C)=\{a\in\mathcal{R}_{1,k}:\text{There exists } b\in\mathcal{R}_{1,k}\ \text{s.t } a+ub\in C\},$$

که یک ایده‌آل چپ $\mathcal{R}_{1,k}$ است. بنا به گزاره ۱۳.۲، $\mathrm{Res}(C)=\mathcal{R}_{1,k}(a_1(x))$ که در آن $a_1(x)$ یک عامل

تکین از x^k-1 است. اگر $\mathcal{I}$ یک ایده‌آل چپ $\mathcal{R}_k$ باشد، آنگاه $\mu(\mathcal{I})=\mathrm{Res}(\mathcal{I})$.

در گزاره‌ی بعدی ایده‌آل‌های چپ $\mathcal{R}_k$ را مشخص می‌کنیم:

گزاره ۱.۳. هر ایده‌آل چپ $\mathcal{R}_k$ به فرم زیر است:

$$\mathcal{I}=\mathcal{R}_k(a_1(x)+ug(x))+\mathcal{R}_k(ua_2(x)),$$

که در آن $a_1(x)$ و $a_2(x)$ عناصری در $\mathcal{F}_k$ هستند به طوری که $a_2(x)|_r a_1(x)$. به‌علاوه، $g(x)$ عنصری در $\mathcal{R}_{1,k}$ از درجه حداکثر $\deg(a_2(x))-1$ است و تحت این شرایط یکتا می‌باشد.

اثبات. از آنجا که $\mathcal{I}$ ایده‌آل چپ از $\mathcal{R}_k$ است، لذا ایده‌آل چپ I از $R_2[x;\Theta]$ شامل $\langle x^k-1\rangle$ موجود است به طوری که $\mathcal{I}=\frac{I}{\langle x^k-1\rangle}$. چون $\mu:R_2[x;\Theta]\to\mathbb{F}_q[x;\theta]$ پوشا است، از این رو $\mu(I)$ ایده‌آل چپ $\mathbb{F}_q[x;\theta]$ است. پس چندجمله‌ای g در $R_2[x;\Theta]$ وجود دارد به طوری که $\mu(I)=\mathbb{F}_{p^m}[x;\theta]\mu(g(x))$. چون $\mu|_I:I\to\mu(I)$ نیز پوشا است، لذا $f\in I$ وجود دارد که $\mu(f)=\mu(g)$. فرض کنیم f_1 عنصر دلخواهی از I باشد. در این صورت $\mu(f_1)\in\mu(I)=\mathbb{F}_q[x;\theta]\mu(f)$. بنابراین چندجمله‌ای h در $R_2[x;\Theta]$ وجود دارد به طوری که

$$\mu(f_1)=\mu(h)\mu(f)=\mu(hf).$$

از این رو $r\in uR_2[x;\Theta]$ وجود دارد که $f_1=hf+r$. از آنجایی که $r=f_1-hf\in I\cap uR_2[x;\Theta]$، داریم

$$f_1=hf+r\in R_2[x;\Theta]f+I\cap uR_2[x;\Theta]$$

و این ایجاب می‌کند

$$I=R_2[x;\Theta]f+I\cap uR_2[x;\Theta].$$

از طرفی $\langle x^k-1\rangle\subseteq I$. پس

$$\mathcal{I}=\frac{I}{\langle x^k-1\rangle}=\frac{R_2[x;\Theta]f+\langle x^k-1\rangle}{\langle x^k-1\rangle}+\left(\frac{I}{\langle x^k-1\rangle}\cap\frac{uR_2[x;\Theta]+\langle x^k-1\rangle}{\langle x^k-1\rangle}\right)=\mathcal{R}_kf+(u\mathcal{R}_k\cap\mathcal{I}).$$

با استفاده از گزاره ۱۳.۲، $\mathcal{R}_{1,k}(\mu(f))=\mu(\mathcal{I})=\mathcal{R}_{1,k}(a_1(x))$ که در آن $a_1(x)$ یک عامل تکین از x^k-1 است. در نتیجه چندجمله‌ای $k(x)$ در حلقه‌ی $\mathcal{R}_{1,k}$ موجود است به طوری که $a_1(x)=k(x)\mu(f)$. از این رو $\mu(f)$ یک عامل از x^k-1 است. بدون کاستن از کلیت می‌توان فرض کرد:

$$f(x)=a_1(x)+ug(x),$$

که در آن $g(x)\in\mathcal{R}_{1,k}$. بنابراین

$$\mathcal{R}_kf=\mathcal{R}_k(a_1(x)+ug(x)).$$

با استفاده از گزاره ۱۳.۲، یک عامل تکین از x^k-1 مانند $a_2(x)$ وجود دارد به طوری که

$$\mu((\mathcal{I}:_{\mathcal{R}_k}u))=\mathrm{Res}((\mathcal{I}:_{\mathcal{R}_k}u))=\mathcal{R}_{1,k}(a_2(x)),$$

و

$$\begin{aligned}u\mathcal{R}_k\cap\mathcal{I}&=u(\mathcal{I}:_{\mathcal{R}_k}u)=u\mu^{-1}(\mu((\mathcal{I}:_{\mathcal{R}_k}u)))\\&=u\mu^{-1}(\mathcal{R}_{1,k}(a_2(x))),\end{aligned}$$

که در آن

$$(\mathcal{I}:_{\mathcal{R}_k}u)=\{f(x)\in\mathcal{R}_k:\ uf(x)\in\mathcal{I}\},$$

و

$$\mu^{-1}(\mu((\mathcal{I}:_{\mathcal{R}_k}u)))=\{g(x)\in\mathcal{R}_k:\ \mu(g(x))\in\mu((\mathcal{I}:_{\mathcal{R}_k}u))\}.$$

همچنین $u\mathcal{R}_{1,k}=u\mathcal{R}_k$. بنابراین $u\mu^{-1}(\mathcal{R}_{1,k}(a_2(x)))=\mathcal{R}_k(ua_2(x))$. به عبارت دیگر

$$\mathcal{I}=\mathcal{R}_k(a_1(x)+ug(x))+\mathcal{R}_k(ua_2(x)).$$

می‌توان فرض کرد $\deg(g(x))<\deg(a_2(x))$، زیرا با استفاده از الگوریتم تقسیم داریم:

$$g(x)=h_1(x)a_2(x)+h_2(x),$$

که در آن $\deg(h_2(x))<\deg(a_2(x))$. لذا

$$a_1(x)+uh_2(x)=a_1(x)+ug(x)-uh_1(x)a_2(x)\in\mathcal{I}.$$

از این رو $\mathcal{I}=\mathcal{R}_k(a_1(x)+uh_2(x))+\mathcal{R}_k(ua_2(x))$. ادعا

می‌کنیم $g(x)$ با شرط $\deg(g(x))<\deg(a_2(x))$، منحصربه‌فرد است. فرض کنیم $g'(x)$ یک چندجمله‌ای با شرط $\deg(g'(x))<\deg(a_2(x))$ باشد به طوری که

$$\mathcal{I}=\mathcal{R}_k(a_1(x)+ug'(x))+\mathcal{R}_k(ua_2(x)).$$

در این صورت

$$u(g(x)-g'(x))\in\mathcal{I}.$$

این نتیجه می‌دهد

$$g(x)-g'(x)=\mu(g(x)-g'(x))\in\mu((\mathcal{I}:_{\mathcal{R}_k}u))=\mathcal{R}_{1,k}(a_2(x)).$$

اگر $g(x)\neq g'(x)$، آنگاه

$$\deg(g(x)-g'(x))\geq\deg(a_2(x))$$

که این با فرض

$$\deg(g(x)-g'(x))<\deg(a_2(x))$$

در تناقض است. در نتیجه $g(x)=g'(x)$. همچنین

$$a_1(x)\in\mathrm{Res}(\mathcal{I})\subseteq\mathrm{Res}((\mathcal{I}:_{\mathcal{R}_k}u))=\mathcal{R}_{1,k}(a_2(x)).$$

از این رو اگر $a_2(x)\neq 0$،آنگاه $a_2(x)|_r a_1(x)$. پس ایده‌آل چپ $\mathcal{I}$ از $\mathcal{R}_k$ به شکل زیر است:

$$\mathcal{I}=\mathcal{R}_k(a_1(x)+ug(x))+\mathcal{R}_k(ua_2(x)),$$

که در آن $\deg(g(x))<\deg(a_2(x))$ و $g(x)$ با این شرایط یکتاست. علاوه بر این، $a_2(x)\neq 0$ ایجاب می‌کند $a_2(x)|_r a_1(x)$.

در قضیه بعدی زیرمدول‌های چپ $\mathcal{R}_{\alpha,\beta}$ را مشخص می‌کنیم که اثبات آن مشابه اثبات قضیه ۱.۳ مرجع [۱] است.

قضیه ۲.۳. هر $R_2[x;\Theta]$–زیرمدول چپ از $\mathcal{R}_{\alpha,\beta}$ به فرم زیر است:

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)|0))+\mathcal{R}_n((u\hat{a}_2(x)|0))$$
$$+\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)|ua_2(x))),$$

که در آن برای $i=1,2$ داریم $\hat{a}_i(x)\in\mathcal{F}_\alpha$، $a_i(x)\in\mathcal{F}_\beta$، $\hat{g}(x)\in\mathcal{R}_{1,\alpha}$، $g(x)\in\mathcal{R}_{1,\beta}$، $0\le\deg(\hat{a}_1(x))\le\alpha$، $\deg(\hat{g}(x))<\deg(\hat{a}_2(x))$، $0\le\deg(a_1(x))\le\beta$، $\deg(g(x))<\deg(a_2(x))$، $\hat{a}_2(x)|_r\hat{a}_1(x)$، $a_2(x)|_r a_1(x)$ و $k_i(x)\in\mathcal{R}_\alpha$. به‌علاوه، $\hat{g}(x)$ و $g(x)$ تحت شرایط فوق یکتا هستند.

لم ۳.۳. اگر

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)|0))+\mathcal{R}_n((u\hat{a}_2(x)|0))$$
$$+\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)|ua_2(x))),$$

یک کد دوری اریب R_2–مضاعف از طول (α,β) باشد، آنگاه می‌توان فرض کرد $\deg(k_1(x))<\deg(\hat{a}_1(x)+u\hat{g}(x))$ و $\deg(k_2(x))<\deg(\hat{a}_1(x)+u\hat{g}(x))$.

اثبات. با استفاده از الگوریتم تقسیم راست، عناصر $q(x)$ و $r(x)$ در $R_2[x;\Theta]$ وجود دارند به‌طوری که

$$k_1(x)=q(x)(\hat{a}_1(x)+u\hat{g}(x))+r(x),$$

که در آن $r(x)=0$ یا $\deg(r(x))<\deg(\hat{a}_1(x)+u\hat{g}(x))$. لذا

$$(r(x)|a_1(x)+ug(x))=(k_1(x)-q(x)(\hat{a}_1(x)+u\hat{g}(x))|a_1(x)+ug(x))$$
$$=(k_1(x)|a_1(x)+ug(x))-q(x)(\hat{a}_1(x)+u\hat{g}(x))|0)\in C.$$

بنابراین

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)|0))+\mathcal{R}_n((u\hat{a}_2(x)|0))$$
$$+\mathcal{R}_n((r(x)|a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)|ua_2(x))).$$

از این رو می‌توانیم فرض کنیم $\deg(k_1(x))<\deg(\hat{a}_1(x)+u\hat{g}(x))$. با روشی مشابه بالا می‌توان نشان داد

$$\deg(k_2(x))<\deg(\hat{a}_1(x)+u\hat{g}(x)).$$

کدهای دوری اریب R_2–مضاعف از طول (α,β) به صورت زیر دسته‌بندی می‌شوند:

قضیه ۴.۳. کدهای دوری اریب R_2–مضاعف از طول (α,β) عبارتند از:

- دسته اول: 0 و $\mathcal{R}_{\alpha,\beta}$.
- دسته دوم: $\mathcal{R}_n((u\hat{a}_2(x)|0))$، که در آن $\hat{a}_2(x)\in\mathcal{F}_\alpha$ و $0\le\deg(\hat{a}_2(x))\le\alpha-1$.
- دسته سوم: $\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)|0))$، که در آن $\hat{a}_1(x)\in\mathcal{F}_\alpha$، $0\le\deg(\hat{a}_1(x))\le\alpha-1$، $\hat{g}(x)\in\mathcal{R}_{1,\alpha}$ و $\deg(\hat{g}(x))<\deg(\hat{a}_1(x))$. به‌علاوه، $\hat{g}(x)$ تحت این شرایط یکتا است.

●دسته چهارم: $\mathcal{R}_n((k_2(x)|ua_2(x)))$، که در آن $k_2(x)\in\mathcal{R}_\alpha$، $a_2(x)\in\mathcal{F}_\beta$ و $0\le \deg(a_2(x))\le \beta-1$.

●دسته پنجم: $\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))$، که در آن $k_1(x)\in\mathcal{R}_\alpha$، $a_1(x)\in\mathcal{F}_\beta$، $0\le\deg(a_1(x))\le\beta-1$ و $g(x)\in\mathcal{R}_{1,\beta}$ و $\deg(g(x))<\deg(a_1(x))$. به‌علاوه، $g(x)$ تحت این شرایط یکتاست.

●دسته ششم:

$\mathcal{R}_n((\hat a_1(x)+u\hat g(x)|0))+\mathcal{R}_n((u\hat a_2(x)|0))$، که در آن $\hat a_1(x)$ و $\hat a_2(x)$ عناصری در $\mathcal{F}_\alpha$ هستند، $0\le\deg(\hat a_1(x))\le\alpha-1$، $\hat a_2(x)|_r \hat a_1(x)$، $\hat g(x)\in\mathcal{R}_{1,\alpha}$ و $\deg(\hat g(x))<\deg(\hat a_2(x))$. به‌علاوه، $\hat g(x)$ تحت شرایط فوق یکتا است.

●دسته هفتم:

$\mathcal{R}_n((\hat a_1(x)+u\hat g(x)|0))+\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))$ که در آن $\hat a_1(x)\in\mathcal{F}_\alpha$، $a_1(x)\in\mathcal{F}_\beta$، $0\le\deg(\hat a_1(x))\le\alpha-1$، $0\le\deg(a_1(x))\le\beta-1$، $k_1(x)\in\mathcal{R}_\alpha$، $\deg(k_1(x))<\deg(\hat a_1(x)+u\hat g(x))$، $\hat g(x)\in\mathcal{R}_{1,\beta}$، $g(x)\in\mathcal{R}_{1,\beta}$، $\deg(\hat g(x))<\deg(\hat a_1(x))$ و $\deg(g(x))<\deg(a_1(x))$. به‌علاوه، $\hat g(x)$ و $g(x)$ تحت شرایط فوق یکتا هستند.

●دسته هشتم:

$\mathcal{R}_n((\hat a_1(x)+u\hat g(x)|0))+\mathcal{R}_n((k_2(x)|ua_2(x)))$ که در آن $\hat a_1(x)$ عنصری در $\mathcal{F}_\alpha$ از درجه حداکثر $\alpha-1$ و $a_2(x)$ عنصری در $\mathcal{F}_\beta$ از درجه حداکثر $\beta-1$ است، $k_2(x)\in\mathcal{R}_\alpha$، $\deg(k_2(x))<\deg(\hat a_1(x)+u\hat g(x))$ $\hat g(x)\in\mathcal{R}_{1,\beta}$ و $\deg(\hat g(x))<\deg(\hat a_1(x))$ به‌علاوه، $\hat g(x)$ تحت این شرایط یکتا است.

●دسته نهم:

$\mathcal{R}_n((u\hat a_2(x)|0))+\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))$ که در آن $\hat a_2(x)\in\mathcal{F}_\alpha$، $a_1(x)\in\mathcal{F}_\beta$، $0\le\deg(\hat a_2(x))\le\alpha-1$، $0\le\deg(a_1(x))\le\beta-1$، $k_1(x)\in\mathcal{R}_\alpha$ و $g(x)\in\mathcal{R}_{1,\beta}$. به‌علاوه، $\deg(g(x))<\deg(a_1(x))$ و $g(x)$ تحت شرایط فوق یکتا است.

●دسته دهم:

$\mathcal{R}_n((u\hat a_2(x)|0))+\mathcal{R}_n((k_2(x)|ua_2(x)))$ که در آن $\hat a_2(x)\in\mathcal{F}_\alpha$، $a_2(x)\in\mathcal{F}_\beta$، $k_2(x)\in\mathcal{R}_\alpha$، $0\le\deg(\hat a_2(x))\le\alpha-1$ و $0\le\deg(a_2(x))\le\beta-1$.

●دسته یازدهم:

$\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)|ua_2(x)))$ که در آن $a_1(x)$ و $a_2(x)$ عناصری در $\mathcal{F}_\beta$ هستند $k_1(x)\in\mathcal{R}_\alpha$، $k_2(x)\in\mathcal{R}_\alpha$، $0\le\deg(a_1(x))\le\beta-1$، $0\le\deg(a_2(x))\le\beta-1$، $a_2(x)|_r a_1(x)$، $g(x)\in\mathcal{R}_{1,\beta}$ و $\deg(g(x))<\deg(a_2(x))$. به‌علاوه، $g(x)$ تحت شرایط فوق یکتا است.

●دسته دوازدهم:

$\mathcal{R}_n((\hat a_1(x)+u\hat g(x)|0))+\mathcal{R}_n((u\hat a_2(x)|0))+\mathcal{R}_n((k_1(x)|a_1(x)+ug(x)))$ که در آن $\hat a_1(x),\hat a_2(x)\in\mathcal{F}_\alpha$، $a_1(x)\in\mathcal{F}_\beta$، $0\le\deg(\hat a_1(x))\le\alpha-1$، $0\le\deg(a_1(x))\le\beta-1$، $\hat a_2(x)|_r\hat a_1(x)$، $k_1(x)\in\mathcal{R}_\alpha$، $\deg(k_1(x))<\deg(\hat a_1(x)+u\hat g(x))$، $\hat g(x)\in\mathcal{R}_{1,\alpha}$ و $g(x)\in\mathcal{R}_{1,\beta}$. همچنین $\deg(\hat g(x))<\deg(\hat a_2(x))$ و $\deg(g(x))<\deg(a_1(x))$. به‌علاوه، $g(x)$ و $\hat g(x)$ تحت شرایط فوق یکتا هستند.

●دسته سیزدهم:

$$\mathcal{R}_n((\hat{a}_۱(x)+u\hat{g}(x)|۰))+\mathcal{R}_n((u\hat{a}_۲(x)|۰))$$
$$+\mathcal{R}_n((k_۲(x)|ua_۲(x)))$$

که در آن $\hat{a}_۱(x)$ و $\hat{a}_۲(x)$ عناصری در $\mathcal{F}_\alpha$ حداکثر از درجه $\alpha-۱$ و $a_۲(x)$ عنصری در $\mathcal{F}_\beta$ حداکثر از درجه $\beta-۱$ است، $\hat{a}_۲(x)|_r\,\hat{a}_۱(x)$، $k_۲(x)\in\mathcal{R}_\alpha$، $\deg(k_۲(x))<\deg(\hat{a}_۱(x)+u\hat{g}(x))$، $\hat{g}(x)\in\mathcal{R}_{۱,\alpha}$ و $\deg(\hat{g}(x))<\deg(\hat{a}_۲(x))$. به‌علاوه، $\hat{g}(x)$ تحت شرایط فوق یکتا است.

●دسته چهاردهم:

$$\mathcal{R}_n((u\hat{a}_۲(x)|۰))+\mathcal{R}_n((k_۱(x)|a_۱(x)+ug(x)))$$
$$+\mathcal{R}_n((k_۲(x)|ua_۲(x)))$$

که در آن $\hat{a}_۲(x)$ عنصری در $\mathcal{F}_\alpha$ از درجه حداکثر $\alpha-۱$، $a_۱(x)$ و $a_۲(x)$ عناصری در $\mathcal{F}_\beta$ از درجه حداکثر $\beta-۱$ هستند، $a_۲(x)|_r\,a_۱(x)$، $k_i(x)\in\mathcal{R}_\alpha$، $g(x)\in\mathcal{R}_{۱,\beta}$ و $\deg(g(x))<\deg(a_۲(x))$. به‌علاوه، $g(x)$ تحت شرایط فوق یکتا است.

●دسته پانزدهم:

$$\mathcal{R}_n((\hat{a}_۱(x)+u\hat{g}(x)|۰))+\mathcal{R}_n((k_۱(x)|a_۱(x)+ug(x)))$$
$$+\mathcal{R}_n((k_۲(x)|ua_۲(x)))$$

که در آن $\hat{a}_۱(x)\in\mathcal{F}_\alpha$، $a_i(x)\in\mathcal{F}_\beta$، $۰\le\deg(\hat{a}_۱(x))\le\alpha-۱$، $۰\le\deg(a_۱(x))\le\beta-۱$، $a_۲(x)|_r\,a_۱(x)$، $k_i(x)\in\mathcal{R}_\alpha$ و $\deg(k_i(x))<\deg(\hat{a}_۱(x)+u\hat{g}(x))$ همچنین $\hat{g}(x)\in\mathcal{R}_{۱,\alpha}$، $g(x)\in\mathcal{R}_{۱,\beta}$ و $\deg(\hat{g}(x))<\deg(\hat{a}_۱(x))$ و $\deg(g(x))<\deg(a_۱(x))$. به‌علاوه، $\hat{g}(x)$ و $g(x)$ تحت شرایط فوق یکتا هستند.

●دسته شانزدهم:

$$\mathcal{R}_n((\hat{a}_۱(x)+u\hat{g}(x)|۰))+\mathcal{R}_n((u\hat{a}_۲(x)|۰))$$
$$+\mathcal{R}_n((r(x)|a_۱(x)+ug(x)))+\mathcal{R}_n((k_۲(x)|ua_۲(x)))$$

که در آن $\hat{a}_i(x)$ عناصری در $\mathcal{F}_\alpha$ از درجه حداکثر $\alpha-۱$ و $a_i(x)$ عناصری در $\mathcal{F}_\beta$ از درجه حداکثر $\beta-۱$ هستند. $\hat{g}(x)\in\mathcal{R}_{۱,\alpha}$، $g(x)\in\mathcal{R}_{۱,\beta}$، $\deg(\hat{g}(x))<\deg(\hat{a}_۲(x))$، $\deg(g(x))<\deg(a_۲(x))$، $\hat{a}_۲(x)|_r\,\hat{a}_۱(x)$، $a_۲(x)|_r\,a_۱(x)$، $k_i(x)\in\mathcal{R}_\alpha$ و $\deg(k_i(x))<\deg(\hat{a}_۱(x)+u\hat{g}(x))$. $(i=۱,۲)$ به‌علاوه، $\hat{g}(x)$ و $g(x)$ تحت شرایط فوق یکتا هستند.

اثبات. فرض کنید C یک $R_۲[x;\Theta]$-زیرمدول چپ از $\mathcal{R}_{\alpha,\beta}$ باشد. با استفاده از قضیه ۲.۳

$$C=\mathcal{R}_n((\hat{a}_۱(x)+u\hat{g}(x)|۰))+\mathcal{R}_n((u\hat{a}_۲(x)|۰))$$
$$+\mathcal{R}_n((k_۱(x)|a_۱(x)+ug(x)))+\mathcal{R}_n((k_۲(x)|ua_۲(x))),$$

که در آن، $a_i(x)\in\mathcal{F}_\beta$، $\hat{a}_i(x)\in\mathcal{F}_\alpha$، $g(x)\in\mathcal{R}_{۱,\beta}$ $\hat{g}(x)\in\mathcal{R}_{۱,\alpha}$، $۰\le\deg(\hat{a}_۱(x))\le\alpha$، $\deg(\hat{g}(x))<\deg(\hat{a}_۲(x))$، $۰\le\deg(a_۱(x))\le\beta$، $\deg(g(x))<\deg(a_۲(x))$، $\hat{a}_۲(x)|_r\,\hat{a}_۱(x)$، $a_۲(x)|_r\,a_۱(x)$، $k_i(x)\in\mathcal{R}_\alpha$ و $\deg(k_i(x))<\deg(\hat{a}_۱(x)+u\hat{g}(x)), i=۱,۲$.

دسته اول: $\deg(\hat{a}_i(x))=\deg(a_i(x))=۰$ نتیجه می‌دهد $\hat{g}(x)=g(x)=k_i(x)=۰$ و لذا $C=R_{\alpha,\beta}$. همچنین اگر $\deg(a_i(x))=\beta$، $\deg(\hat{a}_i(x))=\alpha$ و $\hat{g}(x)=g(x)=k_i(x)=۰$ ایجاب می‌کند $\hat{a}_i(x)=x^\alpha-۱$، $a_i(x)=x^\beta-۱$ و لذا $C=۰$.

دسته دوم: $۰\le\deg(\hat{a}_۲(x))\le\alpha-۱$، $\deg(\hat{a}_۱(x))=\alpha$، $\deg(a_i(x))=\beta$ و $\hat{g}(x)=g(x)=k_i(x)=۰$ نتیجه می‌دهد $\hat{a}_۱(x)=x^\alpha-۱$، $a_i(x)=x^\beta-۱$ و $C=\mathcal{R}_n((u\hat{a}_۲(x)|۰))$.

دسته سوم: $\deg(\hat{a}_۲(x))=\alpha$، $\deg(a_i(x))=\beta$، $۰\le\deg(\hat{a}_۱(x))\le\alpha-۱$ و

$g(x)=k_1(x)=k_2(x)=0$ ایجاب می‌کند $C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))$.

دسته چهارم: $\deg(\hat{a}_i(x))=\alpha$، $\deg(a_1(x))=\beta$، $0\le \deg(a_2(x))\le \beta-1$ و $k_1(x)=\hat{g}(x)=g(x)=0$ نتیجه می‌دهد $C=\mathcal{R}_n((k_2(x)\mid ua_2(x)))$.

دسته پنجم: $\deg(\hat{a}_i(x))=\alpha$، $\deg(a_2(x))=\beta$، $0\le \deg(a_1(x))\le \beta-1$ و $k_2(x)=\hat{g}(x)=0$ ایجاب می‌کند $C=\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x)))$.

دسته ششم: $\deg(a_i(x))=\beta$، $0\le \deg(\hat{a}_i(x))\le \alpha-1$ و $k_i(x)=g(x)=0$ نتیجه می‌دهد

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((u\hat{a}_2(x)\mid 0)).$$

دسته هفتم: $\deg(\hat{a}_2(x))=\alpha$، $\deg(a_2(x))=\beta$، $0\le \deg(\hat{a}_1(x))\le \alpha-1$، $0\le \deg(a_1(x))\le \beta-1$ و $k_2(x)=0$ ایجاب می‌کند

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x))).$$

دسته هشتم: $\deg(\hat{a}_2(x))=\alpha$، $\deg(a_1(x))=\beta$، $0\le \deg(\hat{a}_1(x))\le \alpha-1$، $0\le \deg(a_2(x))\le \beta-1$ و $k_1(x)=g(x)=0$ نتیجه می‌دهد

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

دسته نهم: $\deg(\hat{a}_1(x))=\alpha$، $\deg(a_2(x))=\beta$، $0\le \deg(\hat{a}_2(x))\le \alpha-1$، $0\le \deg(a_1(x))\le \beta-1$ و $\hat{g}(x)=k_2(x)=0$ نتیجه می‌دهد

$$C=\mathcal{R}_n((u\hat{a}_2(x)\mid 0))+\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x))).$$

دسته دهم: $\deg(\hat{a}_1(x))=\alpha$، $\deg(a_1(x))=\beta$، $0\le \deg(\hat{a}_2(x))\le \alpha-1$، $0\le \deg(a_2(x))\le \beta-1$ و $k_1(x)=\hat{g}(x)=g(x)=0$ ایجاب می‌کند

$$C=\mathcal{R}_n((u\hat{a}_2(x)\mid 0))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

دسته یازدهم: $\deg(\hat{a}_i(x))=\alpha$، $0\le \deg(a_1(x))\le \beta-1$، $0\le \deg(a_2(x))\le \beta-1$ و $\hat{g}(x)=0$ نتیجه می‌دهد

$$C=\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

دسته دوازدهم: $\deg(a_2(x))=\beta$، $0\le \deg(\hat{a}_i(x))\le \alpha-1$، $0\le \deg(a_1(x))\le \beta-1$ ایجاب می‌کند

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((u\hat{a}_2(x)\mid 0))+\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x))).$$

دسته سیزدهم: $\deg(a_1(x))=\beta$، $0\le \deg(\hat{a}_i(x))\le \alpha-1$ و $0\le \deg(a_2(x))\le \beta-1$ و $k_1(x)=g(x)=0$ نتیجه می‌دهد

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((u\hat{a}_2(x)\mid 0))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

دسته چهاردهم: $\deg(\hat{a}_1(x))=\alpha$، $0\le \deg(\hat{a}_2(x))\le \alpha-1$، $0\le \deg(a_2(x))\le \beta-1$ و $\hat{g}(x)=0$ ایجاب می‌کند

$$C=\mathcal{R}_n((u\hat{a}_2(x)\mid 0))+\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

دسته پانزدهم: $\deg(\hat{a}_2(x))=\alpha$، $0\le \deg(\hat{a}_1(x))\le \alpha-1$، $0\le \deg(a_i(x))\le \beta-1$ نتیجه می‌دهد

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

دسته شانزدهم: $0\le \deg(\hat{a}_i(x))\le \alpha-1$ و $0\le \deg(a_i(x))\le \beta-1$ نتیجه می‌دهد

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)\mid 0))+\mathcal{R}_n((u\hat{a}_2(x)\mid 0))+\mathcal{R}_n((k_1(x)\mid a_1(x)+ug(x)))+\mathcal{R}_n((k_2(x)\mid ua_2(x))).$$

توجه شود که تمام کدهای دوری اریب مضاعف جدایی‌پذیر روی R_2 در یکی از این شانزده دسته قرار دارند و به جز این دسته‌ها، کدهای دیگری وجود ندارند.

۲.۳ کدهای دوری اریب مضاعف جدایی پذیر روی R_2

در این زیربخش، مجموعه‌ی مولد مینیمال و دوگان کدهای دوری اریب مضاعف جدایی پذیر R_2 از طول (α,β) را محاسبه می‌کنیم. یک کد دوری اریب R_2- مضاعف جدایی‌پذیر از طول (α,β) به صورت زیر خواهد بود:

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)|0))+\mathcal{R}_n((u\hat{a}_2(x)|0))$$
$$+\mathcal{R}_n((0|a_1(x)+ug(x)))+\mathcal{R}_n((0|ua_2(x))).$$

گزاره ۵.۳. فرض کنیم C یک کد دوری اریب R_2 - مضاعف جدایی پذیر از طول (α,β) باشد. مجموعه‌های زیر را تعریف می‌کنیم:

$$A_1=\bigcup_{j=0}^{\alpha-\deg(\hat{a}_1(x))-1}\{x^j.(\hat{a}_1(x)+u\hat{g}(x)|0)\},$$

$$A_2=\bigcup_{j=0}^{\deg(\hat{a}_1(x))-\deg(\hat{g}(x))-1}\{x^j.(u\frac{x^{\alpha}-1}{\hat{a}_1(x)}\hat{g}(x)|0)\},$$

$$A_3=\bigcup_{j=0}^{\alpha-\deg(\hat{a}_2(x))-1}\{x^j.(u\hat{a}_2(x)|0)\},$$

$$A_4=\bigcup_{j=0}^{\beta-\deg(a_1(x))-1}\{x^j.(0|a_1(x)+ug(x))\},$$

$$A_5=\bigcup_{j=0}^{\deg(a_1(x))-\deg(g(x))-1}\{x^j.(0|u\frac{x^{\beta}-1}{a_1(x)}g(x))\},$$

$$A_6=\bigcup_{j=0}^{\beta-\deg(a_2(x))-1}\{x^j.(0|ua_2(x))\}.$$

در این صورت $A_1\cup A_2\cup A_3\cup A_4\cup A_5\cup A_6$ به عنوان مجموعه‌ی مولد مینیمال برای کد C -مدول چپ $R_2[x,\Theta]$ خواهد بود.

اثبات. فرض کنیم $c(x)$ یک کد واژه دلخواه از C باشد. در این صورت چندجمله‌ای‌های $f_1(x)$، $f_2(x)$، $f_3(x)$، $f_4(x)$ در $R_2[x,\Theta]$ وجود دارند به طوری که

$$c(x)=f_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0)+f_2(x)\cdot(u\hat{a}_2(x)|0)$$
$$+f_3(x)\cdot(0|a_1(x)+ug(x))+f_4(x)\cdot(0|ua_2(x)).$$

حال اگر $\deg(f_1(x))\le\alpha-\deg(\hat{a}_1(x))-1$ باشد، آنگاه $f_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0)\in\mathrm{span}(A_1)$ که در آن $\mathrm{span}(A_1)$ مجموعه تمام ترکیبات خطی از عناصر A_1 با ضرایب در $R_2[x,\Theta]$ است. در غیر این صورت، با استفاده از الگوریتم تقسیم عناصر $\hat{q}_1(x)$، $\hat{r}_1(x)$ در $\mathbb{F}_q[x,\theta]$ وجود دارند به‌طوری‌که

$$f_1(x)=\hat{q}_1(x)\cdot\frac{x^{\alpha}-1}{\hat{a}_1(x)}+\hat{r}_1(x),$$

که در آن $\hat{r}_1(x)=0$ یا $\deg(\hat{r}_1(x))\le\alpha-\deg(\hat{a}_1(x))-1$. بنابراین

$$f_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0)=\hat{q}_1(x)\cdot(u\frac{x^{\alpha}-1}{\hat{a}_1(x)}\hat{g}(x)|0)$$
$$+\hat{r}_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0).$$

چون $\deg(\hat{r}_1(x))$ حداکثر $\alpha-\deg(\hat{a}_1(x))-1$ است، لذا $\hat{r}_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0)\in\mathrm{span}(A_1)$

حال اگر $\deg(\hat{q}_1(x))\le\deg(\hat{a}_1(x))-\deg(\hat{g}(x))-1$، آنگاه

$$f_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0)\in\mathrm{span}(A_1\cup A_2)$$

درغیر این‌صورت عناصر $\hat{q}_2(x)$ و $\hat{r}_2(x)$ در $\mathbb{F}_q[x,\theta]$ وجود دارند به‌طوری‌که

$$\hat{q}_1(x)=\hat{q}_2(x)\frac{x^{\alpha}-1}{\mathrm{gcld}(\frac{x^{\alpha}-1}{\hat{a}_1(x)}\hat{g}(x),x^{\alpha}-1)}+\hat{r}_2(x),$$

که در آن $\hat{r}_2(x)=0$ یا $\deg(\hat{r}_2(x))\le\deg(\hat{a}_1(x))-\deg(\hat{g}(x))-1$. لذا

$$\hat{q}_1(x)\cdot(u\frac{x^{\alpha}-1}{\hat{a}_1(x)}\hat{g}(x)|0)=\hat{r}_2(x)\cdot(u\frac{x^{\alpha}-1}{\hat{a}_1(x)}\hat{g}(x)|0),$$

و $f_1(x)\cdot(\hat{a}_1(x)+u\hat{g}(x)|0)\in\mathrm{span}(A_1\cup A_2)$.

اگر $\deg(f_2(x))\le\alpha-\deg(\hat{a}_2(x))-1$ باشد، آنگاه $f_2(x)\cdot(u\hat{a}_2(x)|0)\in\mathrm{span}(A_3)$. در غیر این صورت با استفاده از الگوریتم تقسیم عناصر $\hat{q}(x)$، $\hat{r}(x)$ در $\mathbb{F}_q[x,\theta]$ وجود دارند به طوری که

$$f_2(x)=\hat{q}(x)\frac{x^{\alpha}-1}{\hat{a}_2(x)}+\hat{r}(x),$$

که در آن $\hat{r}(x)=0$ یا

$\deg(\hat{r}(x)) \le \alpha - \deg(\hat{a}_2(x)) - 1$. بنابراین
$f_2(x)\cdot(u\hat{a}_2(x)|0) = \hat{r}(x)\cdot(u\hat{a}_2(x)|0) \in \mathrm{span}(A_3)$.
اگر $\deg(f_3(x)) \le \beta - \deg(a_1(x)) - 1$ باشد، آنگاه $f_3(x)\cdot(0|a_1(x)+ug(x)) \in \mathrm{span}(A_4)$.
در غیر این صورت، با استفاده از الگوریتم تقسیم عناصر $q_1(x)$ و $r_1(x)$ در $\mathbb{F}_q[x,\theta]$ وجود دارند به طوری که

$$f_3(x) = q_1(x)\frac{x^{\beta}-1}{a_1(x)} + r_1(x),$$

که در آن $r_1(x)=0$ یا $\deg(r_1(x)) \le \beta - \deg(a(x)) - 1$. بنابراین

$$f_3(x)\cdot(0|a_1(x)+ug(x)) = q_1(x)\cdot(0|u\frac{x^{\beta}-1}{a_1(x)}g(x)) + r_1(x)\cdot(0|a_1(x)+ug(x)).$$

اگر $\deg(q_1(x)) \le \deg(a_1(x)) - \deg(g(x)) - 1$، آنگاه
$f_3(x)\cdot(a_1(x)+ug(x)|0) \in \mathrm{span}(A_4 \cup A_5)$.
درغیر این صورت عناصر $q_2(x)$ و $r_2(x)$ در $\mathbb{F}_q[x,\theta]$ وجود دارند به‌طوری‌که

$$q_1(x) = q_2(x)\frac{x^{\beta}-1}{\mathrm{gcld}(\frac{x^{\beta}-1}{a_1(x)}g(x), x^{\beta}-1)} + r_2(x),$$

که در آن $r_2(x)=0$ یا $\deg(r_2(x)) \le \deg(a_1(x)) - \deg(g(x)) - 1$.
لذا

$$q_1(x)\cdot(0|u\frac{x^{\beta}-1}{a_1(x)}g(x)) = r_2(x)\cdot(0|u\frac{x^{\beta}-1}{a_1(x)}g(x)|0),$$

و $f_3(x)\cdot(0|a_1(x)+ug(x)) \in \mathrm{span}(A_4 \cup A_5)$.
اگر $\deg(f_4(x)) \le \beta - \deg(a_2(x)) - 1$ باشد، آنگاه
$f_4(x)\cdot(0|ua_2(x)) \in \mathrm{span}(A_6)$. در غیر این صورت با استفاده از الگوریتم تقسیم عناصر $q(x)$ و $r(x)$ در $\mathbb{F}_q[x,\theta]$ وجود دارند به طوری که

$$f_4(x) = q(x)\frac{x^{\beta}-1}{a_2(x)} + r(x),$$

که در آن $r(x)=0$ یا $\deg(r(x)) \le \beta - \deg(a_2(x)) - 1$. بنابراین

$$f_4(x)\cdot(0|ua_2(x)) = r(x)\cdot(0|ua_2(x)) \in \mathrm{span}(A_6).$$

واضح است که مجموعه‌ی $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6$ مینیمال است، در واقع هیچ عنصری از $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6$ به صورت ترکیب خطی از عناصر دیگر نوشته نمی‌شود.

□

گزاره ۶.۳. اگر C یک کد دوری اریب R_2- مضاعف از طول (α,β) باشد، آنگاه $C^{\perp}$ نیز یک کد دوری اریب مضاعف روی R_2 خواهد بود.

اثبات. فرض کنیم C کد دوری اریب مضاعف از طول (α,β) روی R_2 باشد. همچنین فرض کنیم $m=\mathrm{lcm}(\alpha,\beta)$،

$$u=(u_0,u_1,\dots,u_{\alpha-2},u_{\alpha-1}|u'_0,u'_1,\dots,u'_{\beta-2},u'_{\beta-1}) \in C,$$

و

$$v=(v_0,v_1,\dots,v_{\alpha-2},v_{\alpha-1}|v'_0,v'_1,\dots,v'_{\beta-2},v'_{\beta-1}) \in C^{\perp}$$

در این صورت $\rho_{\Theta}^{m-1}(u) \in C$ و

$$\begin{aligned}
0 &= \rho_{\Theta}^{m-1}(u)v \\
&= \Theta^{m-1}(u_1)v_0 + \Theta^{m-1}(u_2)v_1 + \dots + \Theta^{m-1}(u_{\alpha-1})v_{\alpha-2} + \Theta^{m-1}(u_0)v_{\alpha-1} \\
&+ \Theta^{m-1}(u'_1)v'_0 + \Theta^{m-1}(u'_2)v'_1 + \dots + \Theta^{m-1}(u'_{\beta-1})v'_{\beta-2} + \Theta^{m-1}(u'_0)v'_{\beta-1} \\
&= \Theta^{m-1}(u_0)v_{\alpha-1} + \Theta^{m-1}(u'_0)v'_{\beta-1} + \sum_{j=1}^{\alpha-1}\Theta^{m-1}(u_j)v_{j-1} + \sum_{j=1}^{\beta-1}\Theta^{m-1}(u'_j)v'_{j-1}.
\end{aligned}$$

از آنجایی که $o(\Theta)|m$، لذا

$$\begin{aligned}
0 &= \Theta(0) \\
&= \Theta(v_{\alpha-1})u_0 + \Theta(v'_{\beta-1})u'_0 + \sum_{j=1}^{\alpha-1}\Theta(v_{j-1})u_j + \sum_{j=1}^{\beta-1}\Theta(v_{j-1})u_j \\
&= \rho_{\Theta}(v)u
\end{aligned}$$

بنابراین $\rho_{\Theta}(v) \in C^{\perp}$.

قضیه ۷.۳. [۱۰] اگر $C = \mathcal{R}_k(a_1(x)+ug(x)) + \mathcal{R}_k(ua_2(x))$، آنگاه چندجمله‌ای $\mu(x)$ در $\mathcal{R}_{1,k}$ وجود دارد به‌طوری‌که $\mu(x)a_2(x) = \frac{x^{k}-1}{a_1(x)}g(x)$ و

$$C^{\perp}=\mathcal{R}_k\left(\left(\frac{x^k-1}{a_2(x)}-u\mu(x)\right)^*\right)+\mathcal{R}_k\left(u\left(\frac{x^k-1}{a_1(x)}\right)^*\right).$$

قضیه ۸.۳. اگر

$$C=\mathcal{R}_n((\hat{a}_1(x)+u\hat{g}(x)|0))+\mathcal{R}_n((u\hat{a}_2(x)|0))$$
$$+\mathcal{R}_n(0|a_1(x)+ug(x))+\mathcal{R}_n(0|ua_2(x)),$$

یک کد دوری اریب مضاعف جدایی پذیر روی R_2 باشد، آنگاه چندجمله‌ای‌های $f(x)$ در $\mathcal{R}_{1,\alpha}$ و $h(x)$ در $\mathcal{R}_{1,\beta}$ وجود دارند به طوری که

$$C^{\perp}=\mathcal{R}_n\left(\left(\left(\frac{x^{\alpha}-1}{\hat{a}_2(x)}-uf(x)\right)^*|0\right)\right)+\mathcal{R}_n\left(\left(u\left(\frac{x^{\alpha}-1}{\hat{a}_1(x)}\right)^*|0\right)\right)$$
$$+\mathcal{R}_n\left(\left(0|\left(\frac{x^{\beta}-1}{a_2(x)}-uh(x)\right)^*\right)\right)+\mathcal{R}_n\left(\left(0|u\left(\frac{x^{\beta}-1}{a_1(x)}\right)^*\right)\right).$$

اثبات. از آنجایی که کد $C=C_{\alpha}\times C_{\beta}$ جدایی‌پذیر است، لذا $C^{\perp}=C_{\alpha}^{\perp}\times C_{\beta}^{\perp}$. داریم:

$$C_{\alpha}=\mathcal{R}_{\alpha}(\hat{a}_1(x)+u\hat{g}(x))+\mathcal{R}_{\alpha}(u\hat{a}_2(x)),$$

و

$$C_{\beta}=\mathcal{R}_{\beta}(a_1(x)+ug(x))+\mathcal{R}_{\beta}(ua_2(x)).$$

با استفاده از قضیه ۷.۳، چندجمله‌ای‌های $f(x)$ در $\mathcal{R}_{1,\alpha}$ و $h(x)$ در $\mathcal{R}_{1,\beta}$ وجود دارند به‌طوری‌که

$$C_{\alpha}^{\perp}=\mathcal{R}_{\alpha}\left(\left(\frac{x^{\alpha}-1}{\hat{a}_2(x)}-uf(x)\right)^*\right)+\mathcal{R}_{\alpha}\left(u\left(\frac{x^{\alpha}-1}{\hat{a}_1(x)}\right)^*\right),$$

و

$$C_{\beta}^{\perp}=\mathcal{R}_{\beta}\left(\left(\frac{x^{\beta}-1}{a_2(x)}-uh(x)\right)^*\right)+\mathcal{R}_{\beta}\left(\left(u\left(\frac{x^{\beta}-1}{a_1(x)}\right)^*\right)\right).$$

۳.۳ مثال‌ها

در این زیر بخش، چند مثال از کدهای دوری اریب R_2- مضاعف جدایی‌پذیر بهینه از طول (α,β) را ارائه می‌دهیم.

تعریف ۹.۳. نگاشت خطی گری به صورت زیر تعریف می‌شود:

$$\varphi:R_2\rightarrow\mathbb{F}_q^2,$$
$$\varphi(x+uy)=(y,x+y),$$

که x و y عناصری در $\mathbb{F}_q$ هستند.

فرض کنیم $r=a+ub$ و $\hat{r}=\hat{a}+u\hat{b}$ عناصری در R_2 باشند. نگاشت $\psi:R_2\times R_2\rightarrow\mathbb{F}_q^4$ با ضابطه

$$\psi(\hat{r}|r)=(\varphi(\hat{r}),\varphi(r))=(\hat{b},\hat{a}+\hat{b},b,a+b),$$

را تعریف کرده و به صورت زیر توسیع می‌دهیم:

$$\psi:R_2^{\alpha}\times R_2^{\beta}\rightarrow\mathbb{F}_q^{2(\alpha+\beta)}$$
$$\psi((\hat{r}_0,\hat{r}_1,\ldots,\hat{r}_{\alpha-1}|r_0,r_1,\ldots,r_{\beta-1}))=(\varphi(\hat{r}_0,\hat{r}_1,\ldots,\hat{r}_{\alpha-1})),(\varphi(r_0,r_1,\ldots,r_{\beta-1})),$$

که در آن $(\hat{r}_0,\hat{r}_1,\ldots,\hat{r}_{\alpha-1})$ عنصری از R_2^{α} و $(r_0,r_1,\ldots,r_{\beta-1})$ عنصری از R_2^{β} است.

یک کد از طول n، اندازه‌ی M و فاصله همینگ d، (n,M,d)- کد نامیده می‌شود. n، M و d را پارامترهای کد می‌گویند. یک (n,M,d)-کد خوب دارای n کوچک، M بزرگ و d بزرگ است.

تعریف ۱۰.۳. کدی که در آن یکی از پارامترهای n، M و d بر حسب دوتای دیگر بهینه سازی شود، کد بهینه گویند.

تعریف ۱۱.۳. اگر C یک کد خطی با پارامترهای $[n,k,d]$ باشد که در آن

$$k+d=n+1,$$

آنگاه C را کد تفکیک پذیر با بیشترین فاصله (MDS) گویند.

مثال ۱۲.۳. فرض کنیم

$$\mathcal{R}_{\alpha}=\mathcal{R}_{\beta}=\frac{(\mathbb{F}_{16}+u\mathbb{F}_{16})[x;\Theta]}{\langle x^2-1\rangle}$$

و θ نگاشت فروبنیوس $\theta(\alpha)=\alpha^4$ است که در آن $\alpha\in\mathbb{F}_{16}$. واضح است که $o(\theta)=2$. هم چنین فرض کنیم δ ریشه‌ی پانزدهم اولیه‌ی واحد در $\mathbb{F}_{16}$ باشد، یعنی

$$\mathbb{F}_{16}=\{0,\delta,\ldots,\delta^{14},\delta^{15}=1\},$$

به‌علاوه، $(x-\delta^3)(x-\delta^{12})$ یک تجزیه از x^2-1 است. مدول‌های زیر را در نظر می‌گیریم:

$$C=\mathcal{R}_4(((\delta^2+u)x|(x-\delta^{12})+u\delta))\quad(1)$$

در این صورت C و $\psi(C)$ به ترتیب دارای ماتریس‌های مولد زیرند:

$$\begin{bmatrix}0 & \delta^2+u & \delta^{12}+u\delta & 1\end{bmatrix}$$

و

$$\begin{bmatrix}0 & 0 & 1 & 1+\delta^2 & \delta & \delta+\delta^{12} & 0 & 1\\ 0 & 0 & \delta^2 & \delta^2 & \delta^{12} & \delta^{12} & 1 & 1\end{bmatrix}$$

لذا $\psi(C)$ یک کد بهینه با پارامترهای $[8,2,5]$ روی $\mathbb{F}_{16}$است.

(۲)

$$C=\mathcal{R}_4((\delta+\delta^4u+(\delta^3+u)x \mid (x-\delta^{12})+u\delta^2))$$

در این صورت C و $\psi(C)$ به ترتیب دارای ماتریس‌های مولد زیرند:

$$\begin{bmatrix} \delta+\delta^4u & \delta^3+u & \delta^{12}+u\delta^2 & 1 \end{bmatrix}$$

و

$$\begin{bmatrix} \delta^4 & \delta^4+\delta & 1 & 1+\delta^3 & \delta^2 & \delta^2+\delta^{12} & 0 & 1 \\ \delta & \delta & \delta^3 & \delta^3 & \delta^{12} & \delta^{12} & 1 & 1 \end{bmatrix}$$

بنابراین $\psi(C)$ یک کد MDS با پارامترهای $[8,2,7]$ روی $\mathbb{F}_{16}$ است.

(۳)

$$C=\mathcal{R}_4((u(x-\delta^{12})|0)+\mathcal{R}_4((\delta^2+\delta^4u)+(\delta+u)x \,|(x-\delta^3)+u\delta^3))$$

در این صورت C دارای ماتریس مولد

$$\begin{bmatrix} u\delta^{12} & u & 0 & 0 \\ \delta^2+\delta^4u & \delta+u & \delta^3+u\delta^3 & 1 \end{bmatrix}$$

و $\psi(C)$ دارای ماتریس مولد

$$\begin{bmatrix} \delta^{12} & \delta^{12} & 1 & 1 & 0 & 0 & 0 & 0 \\ \delta^4 & \delta^4+\delta^2 & 1 & 1+\delta & \delta^3 & 0 & 0 & 1 \\ \delta^2 & \delta^2 & \delta & \delta & \delta^3 & \delta^3 & 1 & 1 \end{bmatrix}$$

هستند. بنابراین $\psi(C)$ یک کد بهینه با پارامترهای $[8,3,4]$ روی $\mathbb{F}_{16}$ است.

۴ – نتیجه‌گیری

فرض کنیم $R_2=\mathbb{F}_q+u\mathbb{F}_q$، $\theta\in \mathrm{Aut}(\mathbb{F}_q)$ و $\Theta\in \mathrm{Aut}(R_2)$ با ضابطه‌ی $\Theta(a+ub)=\theta(a)+u\theta(b)$ باشد. همچنین فرض کنیم $\mathcal{R}_\alpha=\dfrac{R_2[x,\Theta]}{\langle x^\alpha-1\rangle}$ و $\mathcal{R}_\beta=\dfrac{R_2[x,\Theta]}{\langle x^\beta-1\rangle}$. زیر مجموعه‌ی $C\subseteq \mathcal{R}_\alpha\times\mathcal{R}_\beta$ را یک کد Θ-دوری اریب R_2-مضاعف به طول (α,β) نامند، هرگاه $(\hat{c}_0,\hat{c}_1,\ldots,\hat{c}_{\alpha-2},\hat{c}_{\alpha-1} \mid c_0,c_1,\ldots,c_{\beta-2},c_{\beta-1})$ عنصری در C باشد، آنگاه $(\Theta(\hat{c}_{\alpha-1}),\Theta(\hat{c}_0),\Theta(\hat{c}_1),\ldots,\Theta(\hat{c}_{\alpha-2}) \mid \Theta(c_{\beta-1}),\Theta(c_0),\Theta(c_1),\ldots,\Theta(c_{\beta-2}))$ نیز عنصری در C خواهد بود. در واقع، C یک $R_2[x,\Theta]$-زیرمدول چپ از $\mathcal{R}_\alpha\times\mathcal{R}_\beta$ است. در این مقاله ، ساختار جبری این دسته از کدها را بررسی و مولدهای آنها را مشخص کردیم. این کدهارا بر حسب چندجمله‌ای مولد آنها به ۱۶ دسته‌ی مجزا تقسیم کردیم. در ادامه کدهای Θ- دوری اریب R_2- مضاعف جدایی‌پذیر به طول (α,β) را بررسی کرده، مجموعه‌ی مولد مینیمال و دوگان آنها را محاسبه کردیم. این مطالعات را می‌توان با مشخص کردن دوگان کدهای دوری اریب R_2- مضاعف و بررسی کدهای خود دوگان از این نوع ادامه داد.

فهرست منابع

[۱] باقری س.، محمدی حصاری ر.، رضایی ح.، رضایی ر.، سامعی ک.، کدهای دوری اریب ($\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$) $\mathbb{F}_{p^m}$- جمعی از طول $2p^s$، مجله مدل سازی پیشرفته ریاضی

[۲] Abulrub T., Aydin N., & Seneviratne P., *On θ-cyclic codes over* $\mathbb{F}_2+v\mathbb{F}_2$,Australasian. J. Combin, ۵٤ (۲۰۱۲) ۱۱۵-۱۲٦.

[۳] Abualrub T., Siap I., & Aydin N., $\mathbb{Z}_2\mathbb{Z}_4$-*Additive cyclic code*, IEEE. Trans. Inf. Theory., ٦۰(۳) (۲۰۱٤),۱۵۰۸-۱۵۱٤.

[٤] Aydogdu I., Abualrub T., Siap I., & Aydin N., *On* $\mathbb{Z}_2\mathbb{Z}_4$ [*u*]*-additive codes*, Int. J. Comput. Math., ۹۲(۹) (۲۰۱۵), ۱۸۰٦-۱۸۱٤.

[۵] Borges J., Fernandez Cordoba C., & Ten Valls R., $\mathbb{Z}_2$*-Double cyclic codes*, arXiv preprint, arXiv:۱٤۱۰,۵٦۰٤v۱

[٦] Borges J., Fernandez Cordoba C., & Ten Valls R., *Linear and cyclic codes over direct product of chain rings*, Math. Meth. Appl. Sci., (۲۰۱۷), ٦۵۱۹-٦۵۲۹.

[۷] Boucher D., Geiselmann W., & Ulmer F., *Skew-cyclic codes*, Appl. Algebra Eng. Commun. Comput., ۱۸ (۲۰۰۷), ۳۷۹-۳۸۹.

[۸] Chaussade L., Loidreau P., & Ulmer F., *Skew codes of prescribed distance or rank*, Des. Codes Cryptogr, ۵۰ (۲۰۰۹), ۲٦۷-۲۸٤.

[۹] Dinh H.Q., *Constacyclic codes of length* p^s *over* $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, J. Algebra., ۳۲٤ (۲۰۱۰), ۹٤۰-۹۵۰.

[۱۰] Gao J., Shi M., Wu T., & Fu F., *On double cyclic codes over* $\mathbb{Z}_4$, Finite Fields Appl. ۳۹ (۲۰۱٦) ۲۳۳-۲۵۰.

[۱۱] Hesari R.M., Rezaei R., & Samei K., *On self-dual skew cyclic codes of length* p^s *over* *Discrete Math,* in press. $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$

[۱۲] Jitman S., Ling S., & Udomkavanich P., *Skew constacyclic codes over finite chain ring,* Commun ., ٦ (۲۰۱۲), ۳۹-٦۳.

[۱۳] Mahmoudi S., & Samei K., *SR-Additive codes*, Bull. Korean Math. Soc., ۵٦ (۲۰۱۹), ۱۲۳۵-۱۲۵۵.

[۱٤] McDonald B.R., Finite Rings With Identity, Marcel Dekker, New York, ۱۹۷٤.

[۱۵] Prange E., *Cyclic Error-Correcting Codes in Two Symbols,* Cambridge, MA, Tech. Rep., (۱۹۵۷), ۵۷-۱۰۳.