مجله مدل‌سازی پیشرفته ریاضی
سال ۱۴۰۰، دوره ۱۱، شماره ۴، ص ۶۲۶-۶۲۸

شاپا چاپی: ۸۰۸۸-۲۲۵۱
DOI: 10.22055/JAMM.2021.36684.1900

کدهای دوری اریب $\mathbb{F}_{p^m}(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})$-جمعی از طول $2p^s$

سعید باقری [۱]، رقیه محمدی حصاری [۱]، حامد رضایی [۱]، رشید رضایی [۱]، کریم سامعی [۲] ×،

[۱] دانشکده علوم ریاضی و آمار، دانشگاه ملایر، ایران
[۲] دانشکده علوم پایه، دانشگاه بوعلی سینا، همدان، ایران

دبیر مسئول: مهرداد نامداری

تاریخ دریافت:۱۳۹۹/۱۲/۱ تاریخ پذیرش:۱۴۰۰/۷/۲۸

چکیده: فرض کنیم p یک عدد اول و R_2 حلقه‌ی $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ باشد که $u^2=0$. در این مقاله، ساختار جبری کدهای دوری اریب $R_2\mathbb{F}_{p^m}$-جمعی با طول $2p^s$ را مطالعه می‌کنیم و مجموعه چندجمله‌ای‌های مولد این خانواده از کدها را مشخص می‌کنیم. این کدها به هشت دسته‌ی مجزا از زیرمدول‌ها طبقه‌بندی می‌شوند. در پایان با استفاده از یک نگاشت گری، مثال‌هایی از کدهای دوری اریب $R_2\mathbb{F}_{p^m}$-جمعی از طول $2p^s$ را ارائه می‌دهیم.

واژه‌های کلیدی: حلقه‌های زنجیری، کدهای دوری اریب جمعی، نگاشت گری.

رده‌بندی ریاضی: 94B15; 16S36

۱ مقدمه

کدهای خطی، خانواده خاصی از کدها با ساختار ریاضی غنی‌اند. یکی از مهم‌ترین رده‌های کدهای خطی، خانواده کدهای دوری‌اند. ساختار جبری کدهای دوری استفاده از آنها را آسان‌تر می کند، به‌همین دلیل این کدها از اهمیت زیادی برخوردارند.
در [۱] ساختار جبری کدهای دوری $\mathbb{Z}_2\mathbb{Z}_4$-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 [۲] به معرفی کدهای $\mathbb{Z}_2\mathbb{Z}_2[u]$-جمعی پرداخته شده است و اتحاد مک ویلیامز برای کدهای دوگان آنها به‌کار رفته است. کدهای SR-جمعی برای R-جبر، S در [۷] بررسی شده‌اند و ساختار جبری کدهای دوری SR-جمعی مشخص شده است. بورخز و همکارانش در [۳]، ساختار کدهای خطی و دوری روی حاصل‌ضرب حلقه‌های زنجیری متناهی $\mathcal{R}_1$ و $\mathcal{R}_2$ را بررسی کردند. در واقع، کدهای خطی به‌عنوان زیرمدول‌هایی از $\mathcal{R}_1^\alpha\times\mathcal{R}_2^\beta$ و کدهای دوری به‌عنوان زیر مدول‌هایی از $\mathcal{R}_{\alpha,\beta}=\frac{\mathcal{R}_1[x]}{\langle x^\alpha-1\rangle}\times\frac{\mathcal{R}_2[x]}{\langle x^\beta-1\rangle}$ در نظر گرفته می‌شوند، که در آن α و β اعداد صحیح مثبت‌اند.

در سال‌های اخیر، تحقیقات زیادی روی کدها با طول‌های مختلف روی حلقه‌ی $R_2=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ صورت گرفته است و این نشان می‌دهد که کدها روی R_2 کاربردهای عملی بسیاری دارند و برای مطالعه از اهمیت بالایی برخوردارند.

× نویسنده مسئول مقاله: رایانامه: samei@ipm.ir

دینه، تمام کدهای پایادوری از طول p^s روی $R_۲$ را در [۵] مشخص کرد. کدهای دوری اریب در [۴] بررسی شده‌اند. علاوه بر این، ساختار جبری و خواص اساسی این کدها و دوگان اقلیدسی و هرمیتی آنها در [۶] مطالعه شده است. سبحانی و محمودی در [۸] ساختار جبری برخی از کدهای دوری و پایادوری روی حلقه‌ی $\frac{\mathbb{F}_q[u]}{\langle u^۴\rangle}$ را مطالعه کردند.

در این مقاله، ساختار جبری کدهای دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی با طول $۲p^s$ را مطالعه می‌کنیم و مجموعه چندجمله‌ای‌های مولد این خانواده از کدها را به‌دست‌می‌آوریم. بخش دوم به تعاریف و مفاهیم مقدماتی مورد نیاز در این مقاله اختصاص دارد. در بخش سوم، کدهای دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی را دسته‌بندی می‌کنیم و در پایان چند مثال از این کدها را ارائه می‌دهیم.

۲ تعاریف و مقدمات

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

ایدآل I از حلقه‌ی R ایدآل چپ اصلی نامیده می‌شود، هرگاه عنصر $a\in I$ چنان موجود باشد که

$$I=Ra=\{ra:\ r\in R\}.$$

حلقه‌ی یکدار R را حلقه‌ی ایدآل اصلی چپ گویند، هرگاه هر ایدآل چپ آن اصلی باشد. حلقه‌ی تعویض‌پذیر R موضعی نامیده می‌شود، هرگاه فقط یک ایدآل ماکسیمال داشته باشد. حلقه‌ی R را زنجیری گوییم هرگاه ایدآل‌های آن با رابطه شمول کلاً مرتب شده باشد.

تعریف ۱.۲. فرض کنیم R حلقه‌ی تعویض‌پذیر متناهی و σ یک خود ریختی روی R باشد. در این صورت عمل جمع روی مجموعه‌ی

$$R[x,\sigma]=\{a_۰+a_۱x+a_۲x^۲+\cdots+a_nx^n:\ \ a_i\in R,\ \ n\in\mathbb{N}_۰\},$$

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

گزاره ۲.۲. [۶] فرض کنیم n یک عدد طبیعی، R حلقه‌ی تعویض‌پذیر متناهی، σ یک خودریختی روی R و λ عنصری وارون پذیر 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 ایدآل دو طرفه است.

(۳) n مضربی از مرتبه σ و λ تحت σ پایا است، یعنی $\sigma(\lambda)=\lambda$.

تعریف ۳.۲. کد C با 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 ۴.۲. 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 به‌صورت زیر تعریف می‌شود، بسته باشد.

$$\rho_\sigma:R^n\longrightarrow R^n,$$
$$\rho_\sigma((a_۰,a_۱,...,a_{n-۱}))=(\sigma(a_{n-۱}),\sigma(a_۰),...,\sigma(a_{n-۲})).$$

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

لم ۵.۲. [۶] فرض کنیم $\theta\in\mathrm{Aut}(\mathbb{F}_{p^m})$ و $\eta\in\mathbb{F}_{p^m}^*$. نگاشت

$$\Theta_{\theta,\eta}:\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}\longrightarrow\mathbb{F}_{p^m}+u\mathbb{F}_{p^m},$$

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

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

طبق لم فوق، هر خودریختی از حلقه‌ی $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ به شکل $\Theta_{\theta,\eta}$ خواهد بود. در این مقاله قرار داد 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 ۲.۶ [۹] فرض کنیم f و g چندجمله‌ای‌های اریب روی میدان متناهی $\mathbb{F}_{p^m}$ باشند و $f\neq 0$. در این صورت چندجمله‌ای‌های q و r در $\mathbb{F}_{p^m}[x;\Theta]$ وجود دارند به‌طوری‌که $g=qf+r$ که در آن $r=0$ یا $\deg(r)<\deg(f)$. در واقع، حلقه‌ی $\mathbb{F}_{p^m}[x;\Theta]$ یک حوزه ایدآل اصلی است.

گزاره ۲.۷ [۶] فرض کنیم $f(x)$ و $g(x)$ چندجمله‌ای‌هایی در $\mathbb{F}_{p^m}[x;\Theta]$ باشند به‌طوری‌که $f(x)g(x)$ یک چندجمله‌ای اریب مرکزی و تکین است. در این صورت $f(x)g(x)=g(x)f(x)$.

چون $x^{p^s}-1$ عنصر مرکزی و تکین $\mathbb{F}_{p^m}[x;\Theta]$ است، بنا به گزاره ۲.۷، مقسوم‌علیه‌های راست این عنصر دو طرفه‌اند. حلقه‌ی چندجمله‌ای‌های اریب $\mathbb{F}_{p^m}[x;\Theta]$ حوزه تجزیه یکتا نیست. در واقع ممکن است تجزیه‌های مختلفی برای یک چندجمله‌ای وجود داشته باشد. به عنوان مثال اگر δ ریشه‌ی پانزدهم اولیه‌ی واحد در $\mathbb{F}_{16}$ و θ یک خودریختی از آن با ضابطه

$$\forall\alpha\in\mathbb{F}_{16},\qquad \theta(\alpha)=\alpha^2,$$

باشد، آنگاه $o(\theta)=4$ و

$$x^4-1=(x-1)^4=(x-\delta^{10})(x-\delta^5)(x-\delta^{10})(x-\delta^5),$$

دو تجزیه‌ی متفاوت از x^4-1 در $\mathbb{F}_{16}[x;\Theta]$ اند.

در این مقاله نمادگذاری‌های زیر را به‌کار می‌بریم:

(۱) $\mathbb{F}_{p^m}[x;\Theta]=\mathbb{F}_{p^m}[x;\theta]$.

(۲) $R_2=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$.

(۳) $\mathcal{R}_1=\frac{\mathbb{F}_{p^m}[x;\Theta]}{\langle x^{p^s}-1\rangle}$.

(۴) $\mathcal{R}_2=\frac{R_2[x;\Theta]}{\langle x^{p^s}-1\rangle}$.

(۵) $\mathcal{R}=\mathcal{R}_1\times\mathcal{R}_2$.

همچنین فرض کنیم $p^s\mid l$ که در آن $o(\Theta)=o(\theta)=l$ مرتبه خودریختی Θ است.

همریختی طبیعی $\mu:R_2\longrightarrow\mathbb{F}_{p^m}$ با ضابطه $\mu(a_0+ub_0)=a_0$ را به‌صورت زیر توسیع می‌دهیم:

$$\mu:R_2[x;\Theta]\longrightarrow\mathbb{F}_{p^m}[x;\Theta],$$
$$\sum_{i=0}^{n}(a_i+ub_i)x^i\longmapsto\sum_{i=0}^{n}a_ix^i.$$

همچنین این همریختی می‌تواند به $\mu:\mathcal{R}_2\longrightarrow\mathcal{R}_1$ توسیع یابد.

مجموعه‌ی $\mathbb{F}_{p^m}R_2=\{(a,b):\quad a\in\mathbb{F}_{p^m},b\in R_2\}$ با عمل جمع مولفه‌به‌مولفه یک گروه آبلی است. با تعریف ضرب اسکالر

$$.:R_2\times\mathbb{F}_{p^m}R_2\longrightarrow\mathbb{F}_{p^m}R_2,$$
$$r.(a,b)=(\mu(r)a,rb).$$

می‌توان $\mathbb{F}_{p^m}R_2$ را به یک R_2- مدول تبدیل کرد. حتی با توسیع ضرب اسکالر به‌صورت زیر

$$r.(a_0,a_1,...,a_{n_1-1},b_0,b_1,...,b_{n_2-1})=(\mu(r)a_0,\mu(r)a_1,...,\mu(r)a_{n_1-1},rb_0,rb_1,...,rb_{n_2-1}),$$

می‌توان $\mathbb{F}_{p^m}^{n_1}R_2^{n_2}$ را به یک R_2- مدول تبدیل کرد که $(a_0,a_1,...,a_{n_1-1})$ عنصری از $\mathbb{F}_{p^m}^{n_1}$ و $(b_0,b_1,...,b_{n_2-1})$ عنصری از $R_2^{n_2}$ است.

تعریف ۸.۲. زیر مجموعه‌ی ناتهی C از $\mathbb{F}_{p^m}^{n_1}R_2^{n_2}$ یک کد $\mathbb{F}_{p^m}R_2$-جمعی نامیده می‌شود هرگاه C یک R_2- زیرمدولی از $\mathbb{F}_{p^m}^{n_1}R_2^{n_2}$ باشد.

در این مقاله فرض بر این است که: $n_1=n_2=p^s$.

ملاحظه ۹.۲. فرض کنیم $a=(a_0,a_1,...,a_{p^s-1})\in\mathbb{F}_{p^m}^{p^s}$ و $b=(b_0,b_1,...,b_{p^s-1})\in R_2^{p^s}$. در این صورت نمایش منحصربه‌فرد کد واژه $c=(a,b)\in\mathcal{R}$ بر حسب چندجمله‌ای‌ها به‌صورت زیر است:

$$c(x)=(a_0+a_1x+\cdots+a_{p^s-1}x^{p^s-1},b_0+b_1x+\cdots+b_{p^s-1}x^{p^s-1})=(a(x),b(x))\in\mathcal{R}.$$

حال فرض کنیم $(f(x),g(x))$ عنصری در $\mathcal{R}$ و $r(x)$ عنصری در $R_2[x;\Theta]$ باشد. در این صورت ضرب اسکالر "." که در بالا تعریف شد، به‌صورت زیر خواهد بود:

$$\begin{aligned}&.:R_2[x;\Theta]\times\mathcal{R}\longrightarrow\mathcal{R},\\&r(x).(f(x),g(x))=(\mu(r(x))f(x),r(x)g(x)),\end{aligned}$$

که در آن

$$\mu(r(x))=\mu(\sum_{j=0}^{p^s-1}r_jx^j)=\sum_{j=0}^{p^s-1}\mu(r_j)x^j,$$

و $r_j\in R_2$.

توجه داشته باشید که میدان $\mathbb{F}_{p^m}$ زیرحلقه‌ای از R_2 است. به‌علاوه، R_2 با $\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}$ به‌عنوان گروه جمعی یکریخت است. با توجه به مطالب فوق، لم زیر را داریم:

لم ۱۰.۲. C یک کد دوری اریب $\mathbb{F}_{p^m}R_2$-جمعی است اگر و تنها اگر C یک $R_2[x;\Theta]$- زیرمدول چپ از $\mathcal{R}$ باشد.

نگاشت گری φ را به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned}&\varphi:R_2^{p^s}\longrightarrow\mathbb{F}_{p^m}^{2p^s},\\&\varphi(x+uy)=(y,x+y),\end{aligned}$$

که x و y عناصری در $\mathbb{F}_{p^m}^{p^s}$ اند. همچنین فرض کنیم $r=a+ub\in R_2, d\in\mathbb{F}_{p^m}$. نگاشت $\psi:\mathbb{F}_{p^m}R_2\longrightarrow\mathbb{F}_{p^m}^{3}$ با ضابطه $\psi(d,r)=(d,\varphi(r))=(d,b,a+b)$ را به‌صورت زیر توسیع می‌دهیم:

$$\begin{aligned}&\psi:\mathbb{F}_{p^m}^{p^s}R_2^{p^s}\longrightarrow\mathbb{F}_{p^m}^{3p^s},\\&\psi(d_0,d_1,...,d_{p^s-1},r_0,r_1,...,r_{p^s-1})=(d_0,d_1,...,d_{p^s-1},\varphi((r_0,r_1,...,r_{p^s-1}))),\end{aligned}$$

که در آن $(d_0,d_1,...,d_{p^s-1})$ عنصری از $\mathbb{F}_{p^m}^{p^s}$ و $(r_0,r_1,...,r_{p^s-1})$ عنصری از $R_2^{p^s}$ است.

حال اگر C یک کد دوری اریب $\mathbb{F}_{p^m}R_2$-جمعی از طول $2p^s$ باشد، آنگاه $\mathcal{C}=\psi(C)$ کد دوری اریب از طول $3p^s$ روی $\mathbb{F}_{p^m}$ خواهد بود.

لم ۱۱.۲. [۵] C یک کد دوری اریب از طول p^s روی $\mathbb{F}_{p^m}$ است اگر و تنها اگر C یک ایدآل چپ $\mathcal{R}_1$ باشد.

در گزاره بعدی، ساختار جبری کدهای دوری اریب از طول p^s روی $\mathbb{F}_{p^m}$ را مشخص می‌کنیم.

گزاره ۱۲.۲. $\mathcal{R}_1$ حلقه‌ی ایدآل اصلی چپ است و ساختار ایدآل‌های چپ آن به‌صورت $\mathcal{R}_1\big(a(x)\big)$ است که در آن $a(x)$ یک عامل تکین از $x^{p^s}-1$ است.

اثبات. فرض کنیم $\frac{I}{\langle x^{p^s}-۱\rangle}$ ایدآل چپ حلقه‌ی $\mathcal{R}_۱$ باشد که در آن I ایدآل چپ $\mathbb{F}_{p^m}[x;\Theta]$ شامل $\langle x^{p^s}-۱\rangle$ است. در این صورت $f(x)\in\mathbb{F}_{p^m}[x;\Theta]$ وجود دارد به‌طوری‌که $I=\mathbb{F}_{p^m}[x;\Theta]f(x)$ و $f(x)\mid x^{p^s}-۱$. کافی است قرار دهیم $a(x)=f(x)+\langle x^{p^s}-۱\rangle$.

□

حلقه‌ی $R_۲=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ یک حلقه‌ی زنجیری متناهی با درجه پوچی ۲ است. همچنین مشخصه‌ی این حلقه برابر p و $u\mathbb{F}_{p^m}$ تنها ایدآل ماکسیمال آن است. کدهای دوری اریب از طول p^s روی $R_۲$، ایدآل‌های چپ $\mathcal{R}_۲$ اند.

فرض کنیم C یک کد دوری اریب از طول p^s روی $R_۲$ باشد. در این صورت کد کاهش یافته از C را به‌صورت زیر تعریف می‌کنیم:

$$\mathrm{Res}(C)=\{a\in\mathcal{R}_۱:\quad \exists\, b\in\mathcal{R}_۱\ \ \mathrm{s.t}\ \ a+ub\in C\},$$

که ایدآل چپ $\mathcal{R}_۱$ است. بنا بر گزاره ۱۲.۲، $\mathrm{Res}(C)=\mathcal{R}_۱\big(a_۱(x)\big)$ که در آن $a_۱(x)$ یک عامل تکین از $x^{p^s}-۱$ است. اگر $\mathcal{I}$ یک ایدآل چپ $\mathcal{R}_۲$ باشد، آنگاه $\mu(\mathcal{I})=\mathrm{Res}(\mathcal{I})$.

ملاحظه ۱۳.۲. با روندی مشابه [۵] می‌توان نشان داد که هر چندجمله‌ای دلخواه $f(x)$ در $\mathcal{R}_۲$، دارای نمایش منحصربه‌فرد

$$f(x)=\sum_{j=۰}^{p^s-۱}a_{۰j}(x-۱)^j+u\sum_{j=۰}^{p^s-۱}a_{۱j}(x-۱)^j,$$

است که در آن $a_{۱j},a_{۰j}$ عناصری در $\mathbb{F}_{p^m}$ اند.

۳ نتایج اصلی

۱.۳ کدهای دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی

در این زیربخش، ساختار جبری کدهای دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی از طول $۲p^s$ را مطالعه می‌کنیم و مجموعه مولدهای این دسته از کدها را به عنوان $R_۲[x;\Theta]$- زیرمدول‌های چپ $\mathcal{R}$ مشخص می‌کنیم.

فرض کنیم C یک کد دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی از طول $۲p^s$ باشد. نگاشت

$$\begin{aligned}&\phi: C\longrightarrow \mathcal{R}_۲,\\ &\phi(a(x),b(x))=b(x),\end{aligned}$$

یک همریختی $R_۲[x;\Theta]$–مدولی است. در این صورت $\mathrm{Im}(\phi)$ زیرمدولی از $\mathcal{R}_۲$ و همچنین $\mathrm{Ker}(\phi)$ زیرمدولی از C خواهد بود. به‌علاوه، $\mathrm{Im}(\phi)$ یک ایدآل چپ $\mathcal{R}_۲$ است.

در قضیه زیر، مولد کدهای دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی از طول $۲p^s$ را مشخص می‌کنیم.

قضیه ۱.۳. کدهای دوری اریب $\mathbb{F}_{p^m}R_۲$–جمعی از طول $۲p^s$ به صورت زیر دسته‌بندی می‌شوند:

دسته اول: کدهای بدیهی $C=۰$ و $C=\mathcal{R}$.

دسته دوم: $C=\mathcal{R}_۲\big((a(x),۰)\big)$ که در آن $a(x)$ یک عامل تکین از $(x-۱)^{p^s}$ است و $۰\le\deg(a(x))\le p^s-۱$.

دسته سوم: $C=\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)$ که در آن $a_۱(x)$ یک عامل تکین از $(x-۱)^{p^s}$ از درجه حداکثر $p^s-۱$ است، $g_۱(x)$ و $g(x)$ عناصری در $\mathcal{R}_۱$ اند که $\deg(g(x))<\deg(a_۱(x))$. به‌علاوه، $g(x)$ با این شرایط یکتا است.

دسته چهارم: $C=\mathcal{R}_۲\big((g_۲(x),ua_۲(x))\big)$ که در آن $a_۲(x)$ یک عامل تکین از $(x-۱)^{p^s}$ از درجه حداکثر $p^s-۱$ است و $g_۲(x)$ عنصری در $\mathcal{R}_۱$ است.

دسته پنجم: $C=\mathcal{R}_۲\big((a(x),۰)\big)+\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)$ که در آن $a(x)$ و $a_۱(x)$ عامل‌های تکین از

$(x-1)^{p^s}$ از درجه حداکثر p^s-1 اند. به‌علاوه، $g_1(x)$ و $g(x)$ عناصری در $\mathcal{R}_1$ هستند که $\deg(g_1(x))<\deg(a(x))$.

دسته ششم: $C=\mathcal{R}_2\big((a(x),0)\big)+\mathcal{R}_2\big((g_2(x),ua_2(x))\big)$ که در آن $a(x)$ و $a_2(x)$ عامل‌های تکین از $(x-1)^{p^s}$ از درجه حداکثر p^s-1 اند. به‌علاوه، $g_2(x)$ عنصری در $\mathcal{R}_1$ است که $\deg(g_2(x))<\deg(a(x))$.

دسته هفتم: $C=\mathcal{R}_2\big((g_1(x),a_1(x)+ug(x))\big)+\mathcal{R}_2\big((g_2(x),ua_2(x))\big)$ که در آن $a_1(x)$ و $a_2(x)$ عامل‌های تکین از $(x-1)^{p^s}$ از درجه حداکثر p^s-1 به گونه‌ای‌اند که $a_2(x)\mid_r a_1(x)$، همچنین $g_1(x)$، $g(x)$ و $g_2(x)$ عناصری در $\mathcal{R}_1$ اند. به‌علاوه، $g(x)$ با این شرایط یکتا است.

دسته هشتم: $C=\mathcal{R}_2\big((a(x),0)\big)+\mathcal{R}_2\big((g_1(x),a_1(x)+ug(x))\big)+\mathcal{R}_2\big((g_2(x),ua_2(x))\big)$ که در آن $a(x)$ و $a_1(x)$ و $a_2(x)$ عامل‌های تکین از $(x-1)^{p^s}$ از درجه حداکثر p^s-1 اند و $a_2(x)\mid_r a_1(x)$، همچنین $g_1(x)$ و $g(x)$ و $g_2(x)$ عناصری در $\mathcal{R}_1$ اند که $\deg(g_1(x))<\deg(a(x))$ و $\deg(g_2(x))<\deg(a(x))$. به‌علاوه، $g(x)$ با این شرایط یکتا است.

اثبات. طبق آنچه در بالا گفته شد $\mathcal{I}=\mathrm{Im}(\phi)$ یک ایدآل چپ $\mathcal{R}_2$ است. ابتدا ساختار $\mathcal{I}$ را مشخص می‌کنیم. ایدآل چپ I از $R_2[x;\Theta]$ شامل $\langle(x-1)^{p^s}\rangle$ موجود است به‌طوری‌که $\mu:R_2[x;\Theta]\longrightarrow\mathbb{F}_{p^m}[x;\Theta]$ پوشا است، از این رو $\mu(I)$ ایدآل چپ $\mathbb{F}_{p^m}[x;\Theta]$ است. پس چندجمله‌ای g در $R_2[x;\Theta]$ وجود دارد به‌طوری‌که $\mu(I)=\mathbb{F}_{p^m}[x;\Theta]\mu(g(x))$. $\mathcal{I}=\frac{I}{\langle(x-1)^{p^s}\rangle}$. چون $\mu|_I:I\longrightarrow\mu(I)$ نیز پوشا است، لذا $f\in I$ وجود دارد که $\mu(f)=\mu(g)$. فرض کنید f_1 عنصر دلخواهی از I باشد. در این صورت $\mu(f_1)\in\mu(I)=\mathbb{F}_{p^m}[x;\Theta]\mu(f)$. بنابراین چندجمله‌ای h در $R_2[x;\Theta]$ وجود دارد به‌طوری‌که

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

از این رو $r\in uR_2[x;\Theta]$ وجود دارد که $f_1=hf+r$. از آنجایی‌که $r=f_1-hf\in I\cap uR_2[x;\Theta]$، داریم $I=R_2[x;\Theta]f+(I\cap uR_2[x;\Theta])$ و این ایجاب می‌کند $f_1=hf+r\in R_2[x;\Theta]f+(I\cap uR_2[x;\Theta])$. از طرفی $\langle(x-1)^{p^s}\rangle\subseteq I$. پس

$$\begin{aligned}\mathcal{I}=\frac{I}{\langle(x-1)^{p^s}\rangle}&=\frac{R_2[x;\Theta]f+\langle(x-1)^{p^s}\rangle}{\langle(x-1)^{p^s}\rangle}+\Big(\frac{I}{\langle(x-1)^{p^s}\rangle}\cap\frac{uR_2[x;\Theta]+\langle(x-1)^{p^s}\rangle}{\langle(x-1)^{p^s}\rangle}\Big)\\&=\mathcal{R}_2f+(u\mathcal{R}_2\cap\mathcal{I}).\end{aligned}$$

با استفاده از گزاره ۱۲.۲، $\mathcal{R}_1\big(\mu(f)\big)=\mu(\mathcal{I})=\mathcal{R}_1\big(a_1(x)\big)$ که در آن $a_1(x)$ یک عامل تکین از $x^{p^s}-1$ است. در نتیجه چندجمله‌ای $k(x)$ در حلقه‌ی $\mathcal{R}_1$ موجود است به‌طوری‌که $a_1(x)=k(x)\mu(f)$. از این رو $\mu(f)$ یک عامل از $x^{p^s}-1$ است. بدون کاستن از کلیت می‌توان فرض کرد:

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

که در آن $g(x)\in\mathcal{R}_1$. بنابراین

$$\mathcal{R}_2f=\mathcal{R}_2\big(a_1(x)+ug(x)\big).$$

با استفاده از گزاره ۱۲.۲، یک عامل تکین از $(x-1)^{p^s}$ مانند $a_2(x)$ وجود دارد به‌طوری‌که

$$\mu((\mathcal{I}:_{\mathcal{R}_2}u))=\mathrm{Res}((\mathcal{I}:_{\mathcal{R}_2}u))=\mathcal{R}_1\big(a_2(x)\big),$$

و

$$u\mathcal{R}_2\cap\mathcal{I}=u(\mathcal{I}:_{\mathcal{R}_2}u)=u\mu^{-1}(\mu((\mathcal{I}:_{\mathcal{R}_2}u)))=u\mu^{-1}(\mathcal{R}_1\big(a_2(x)\big)).$$

همچنین $u\mathcal{R}_1=u\mathcal{R}_2$. بنابراین $u\mu^{-1}(\mathcal{R}_1\big(a_2(x)\big))=\mathcal{R}_2\big(ua_2(x)\big)$. به‌عبارت دیگر

$$\mathcal{I}=\mathcal{R}_2\big(a_1(x)+ug(x)\big)+\mathcal{R}_2\big(ua_2(x)\big).$$

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 $\mathcal{I} = \mathcal{R}_۲\big(a_۱(x) + uh_۲(x)\big) + \mathcal{R}_۲\big(ua_۲(x)\big)$ ادعا می کنیم $g(x)$ با شرط $\deg(g(x)) < \deg(a_۲(x))$، منحصربه‌فرد است. فرض کنیم $g'(x)$ یک چندجمله‌ای با شرط $\deg(g'(x)) < \deg(a_۲(x))$ باشد به‌طوری‌که

$$\mathcal{I} = \mathcal{R}_۲\big(a_۱(x) + ug'(x)\big) + \mathcal{R}_۲\big(ua_۲(x)\big).$$

در این صورت

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

این نتیجه می‌دهد

$$g(x) - g'(x) = \mu(g(x) - g'(x)) \in \mu((\mathcal{I} :_{\mathcal{R}_۲} u)) = \mathcal{R}_۱\big(a_۲(x)\big).$$

اگر $g(x) \neq g'(x)$، آنگاه $\deg(g(x) - g'(x)) \geq \deg(a_۲(x))$، که این با فرض

$$\deg(g(x) - g'(x)) < \deg(a_۲(x))$$

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

$$a_۱(x) \in \mathrm{Res}(\mathcal{I}) \subseteq \mathrm{Res}((\mathcal{I} :_{\mathcal{R}_۲} u)) = \mathcal{R}_۱\big(a_۲(x)\big).$$

از این رو اگر $a_۲(x) \neq ۰$، آنگاه $a_۲(x) \mid_r a_۱(x)$. پس ایدآل چپ $\mathcal{I}$ از $\mathcal{R}_۲$ به شکل زیر است:

$$\mathcal{I} = \mathcal{R}_۲\big(a_۱(x) + ug(x)\big) + \mathcal{R}_۲\big(ua_۲(x)\big),$$

که در آن $\deg(g(x)) < \deg(a_۲(x))$ و $g(x)$ با این شرایط یکتا است. علاوه بر این، $a_۲(x) \neq ۰$ ایجاب می‌کند $a_۲(x) \mid_r a_۱(x)$. از طرفی داریم:

$$\mathrm{Ker}(\phi) = \{(\nu(x), ۰) \in C : \quad \nu(x) \in \mathcal{R}_۱\}.$$

مجموعه J را به صورت زیر تعریف می‌کنیم:

$$J = \{\nu(x) \in \mathcal{R}_۱ : \quad (\nu(x), ۰) \in \mathrm{Ker}(\phi)\}.$$

J یک ایدآل چپ از $\mathcal{R}_۱$ است. در نتیجه بنا به گزاره ۱۲.۲، $J = \mathcal{R}_۱\big(a(x)\big)$ که در آن $a(x)$ یک عامل تکین از $(x-۱)^{p^s}$ است. فرض کنیم $(c_۱(x), ۰)$ عنصر دلخواهی از $\mathrm{Ker}(\phi)$ باشد. در این صورت $c_۱(x) \in J = \mathcal{R}_۱\big(a(x)\big)$. از این رو چندجمله‌ای $k(x)$ در $\mathcal{R}_۱$ وجود دارد به‌طوری‌که $c_۱(x) = k(x)a(x)$. در نتیجه

$$(c_۱(x), ۰) = k(x)(a(x), ۰).$$

پس $\mathrm{Ker}(\phi)$ یک زیرمدول چپ از C است که توسط عنصر $(a(x), ۰)$ تولید می‌شود. با استفاده از قضیه اول یکریختی‌ها داریم:

$$\frac{C}{\mathrm{Ker}(\phi)} \cong \mathrm{Im}(\phi) = \mathcal{R}_۲\big(a_۱(x) + ug(x)\big) + \mathcal{R}_۲\big(ua_۲(x)\big).$$

عناصر $(g_۱(x), a_۱(x) + ug(x))$ و $(g_۲(x), ua_۲(x))$ در C موجودند به‌طوری‌که

$$\phi((g_۱(x), a_۱(x) + ug(x)) = a_۱(x) + ug(x),$$

و

$$\phi((g_۲(x), ua_۲(x))) = ua_۲(x).$$

بنابراین

$$\begin{aligned}
&\phi(\mathcal{R}_۲\big((g_۱(x), a_۱(x) + ug(x))\big) + \mathcal{R}_۲\big((g_۲(x), ua_۲(x))\big)) \\
&= \phi(\mathcal{R}_۲\big((g_۱(x), a_۱(x) + ug(x))\big)) + \phi(\mathcal{R}_۲\big((g_۲(x), ua_۲(x))\big)) \\
&= \mathcal{R}_۲\big(a_۱(x) + ug(x)\big) + \mathcal{R}_۲\big(ua_۲(x)\big),
\end{aligned}$$

از این رو هر کد دوری اریب $R_۲$-$\mathbb{F}_{p^m}$-جمعی از طول $۲p^s$ توسط سه عنصر زیر تولید می‌شود:

$$(a(x),۰),\ (g_۱(x),a_۱(x)+ug(x)),\ (g_۲(x),ua_۲(x)).$$

در واقع

$$C=\mathcal{R}_۲\big((a(x),۰)\big)+\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)+\mathcal{R}_۲\big((g_۲(x),ua_۲(x))\big).$$

مشابه آنچه در بالا برای $g(x)$ گفته شد، می‌توان فرض کرد $\deg(g_۱(x))<\deg(a(x))$ و $\deg(g_۲(x))<\deg(a(x))$.
با در نظر گرفتن حالت‌های مختلف برای چندجمله‌ای‌های $a(x)$ و $a_i(x)$ و $g_i(x)$ و $g(x)$، کد C را می‌توان به هشت دسته‌ی مجزا تقسیم‌بندی کرد:

دسته اول: دو حالت زیر را داریم:

حالت اول: اگر $\deg(a(x))=\deg(a_۱(x))=\deg(a_۲(x))=۰$، آنگاه $g_۱(x)=g(x)=g_۲(x)=۰$ و $C=\mathcal{R}$.

حالت دوم: اگر $\deg(a(x))=\deg(a_۱(x))=\deg(a_۲(x))=p^s$ و $g_۱(x)=g(x)=g_۲(x)=۰$، آنگاه $a(x)=a_۱(x)=a_۲(x)=(x-۱)^{p^s}$ و $C=۰$.

دسته دوم: اگر $۰\leq\deg(a(x))\leq p^s-۱$، $\deg(a_۱(x))=\deg(a_۲(x))=p^s$ و $g_۱(x)=g(x)=g_۲(x)=۰$، آنگاه $a_۱(x)=a_۲(x)=(x-۱)^{p^s}$ و $C=\mathcal{R}_۲\big((a(x),۰)\big)$.

دسته سوم: اگر $\deg(a(x))=\deg(a_۲(x))=p^s$، $۰\leq\deg(a_۱(x))\leq p^s-۱$ و $g_۲(x)=۰$، آنگاه $a(x)=a_۲(x)=(x-۱)^{p^s}$ و $C=\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)$.

دسته چهارم: اگر $\deg(a(x))=\deg(a_۱(x))=p^s$، $۰\leq\deg(a_۲(x))\leq p^s-۱$ و $g_۱(x)=g(x)=۰$، آنگاه $C=\mathcal{R}_۲\big((g_۲(x),ua_۲(x))\big)$.

دسته پنجم: اگر $۰\leq\deg(a(x))\leq p^s-۱$، $\deg(a_۲(x))=p^s$، $۰\leq\deg(a_۱(x))\leq p^s-۱$ و همچنین $g_۲(x)=۰$، آنگاه $C=\mathcal{R}_۲\big((a(x),۰)\big)+\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)$.

دسته ششم: اگر $۰\leq\deg(a(x))\leq p^s-۱$، $\deg(a_۱(x))=p^s$، $۰\leq\deg(a_۲(x))\leq p^s-۱$ و همچنین $g_۱(x)=g(x)=۰$، آنگاه $C=\mathcal{R}_۲\big((a(x),۰)\big)+\mathcal{R}_۲\big((g_۲(x),ua_۲(x))\big)$.

دسته هفتم: اگر $\deg(a(x))=p^s$ و $۰\leq\deg(a_۱(x))\leq p^s-۱$، آنگاه

$$C=\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)+\mathcal{R}_۲\big((g_۲(x),ua_۲(x))\big).$$

دسته هشتم: اگر $۰\leq\deg(a(x))\leq p^s-۱$ و $۰\leq\deg(a_۱(x))\leq p^s-۱$، آنگاه

$$C=\mathcal{R}_۲\big((a(x),۰)\big)+\mathcal{R}_۲\big((g_۱(x),a_۱(x)+ug(x))\big)+\mathcal{R}_۲\big((g_۲(x),ua_۲(x))\big).$$

□

با توجه به قضیه قبل، می‌توان ساختار کدهای دوری $R_۲$-$\mathbb{F}_{p^m}$-جمعی از طول $۲p^s$ را با در نظر گرفتن Θ به‌عنوان نگاشت همانی به‌صورت زیر مشخص کرد:

نتیجه ۲.۳. کدهای دوری $R_۲$-$\mathbb{F}_{p^m}$-جمعی از طول $۲p^s$ به‌صورت زیرند:

دسته اول: کدهای بدیهی $C=۰$ و $C=\mathcal{R}$.

دسته دوم: $C=\mathcal{R}_۲\big(((x-۱)^\nu,۰)\big)$ که در آن $۰\leq\nu\leq p^s-۱$ است.

دسته سوم: $C=\mathcal{R}_۲\big((g_۱(x),(x-۱)^i+uh(x)(x-۱)^t)\big)$ که در آن $g_۱(x)$ عنصری در $\mathcal{R}_۱$ است و $۰\leq i\leq p^s-۱$ و $۰\leq t<i$. به‌علاوه، $h(x)$ یا صفر یا یکه است و نمایشی منحصربه‌فرد به‌صورت $h(x)=\sum_{j=۰}^{i-t-۱}h_j(x-۱)^j$ دارد که در آن $h_j\in\mathbb{F}_{p^m}$ و $h_۰\neq۰$.

دسته چهارم: $C=\mathcal{R}_۲\big((g_۲(x),u(x-۱)^\omega)\big)$ که در آن $g_۲(x)$ عنصری در $\mathcal{R}_۱$ است و $۰\leq\omega\leq p^s-۱$.

دسته پنجم: $C=\mathcal{R}_۲\big(((x-۱)^\nu,۰)\big)+\mathcal{R}_۲\big((g_۱(x),(x-۱)^i+uh(x)(x-۱)^t)\big)$ که در آن $۰\leq\nu\leq p^s-۱$،

$۰ \leq i \leq p^s - ۱$، $۰ \leq t < i$ و $g_۱(x)$ عنصری در $\mathcal{R}_۱$ است. به‌علاوه، $\deg(g_۱(x)) < \nu$ و $h(x)$ مشابه چندجمله‌ای در دسته‌بندی سوم است.

دسته ششم: $C = \mathcal{R}_۲\big(((x-۱)^\nu, ۰)\big) + \mathcal{R}_۲\big((g_۲(x), u(x-۱)^\omega)\big)$ که در آن $۰ \leq \nu \leq p^s - ۱$ و $g_۲(x)$ عنصری در $\mathcal{R}_۱$ است و $\deg(g_۲(x)) < \nu$. به‌علاوه، $۰ \leq \omega \leq p^s - ۱$.

دسته هفتم: $C = \mathcal{R}_۲\big((g_۱(x), (x-۱)^i + uh(x)(x-۱)^t)\big) + \mathcal{R}_۲\big((g_۲(x), u(x-۱)^\omega)\big)$ که در آن $۰ \leq i \leq p^s - ۱$، $۰ \leq t < \omega \leq i$ و $h(x)$ مشابه چندجمله‌ای در دسته‌بندی سوم است که $\deg(h(x)) < \omega - t$. به‌علاوه، $g_۱(x)$ و $g_۲(x)$ عناصری در $\mathcal{R}_۱$ اند که درجه آنها از ν اکیداً کمتر است.

دسته هشتم: $C = \mathcal{R}_۲\big(((x-۱)^\nu, ۰)\big) + \mathcal{R}_۲\big((g_۱(x), (x-۱)^i + uh(x)(x-۱)^t)\big) + \mathcal{R}_۲\big((g_۲(x), u(x-۱)^\omega)\big)$ که در آن $۰ \leq \nu \leq p^s - ۱$، $۰ \leq i \leq p^s - ۱$ و $۰ \leq t < \omega \leq i$ و $h(x)$ مشابه چندجمله‌ای در دسته‌بندی سوم است که $\deg(h(x)) < \omega - t$. به‌علاوه، $g_۱(x)$ و $g_۲(x)$ عناصری در $\mathcal{R}_۱$ اند که درجه آنها از ν اکیداً کمتر است.

۲.۳ مثال ها

در این زیربخش، چند مثال از کدهای دوری اریب $R_۲$-$\mathbb{F}_{p^m}$-جمعی بهینه از طول $۲p^s$ را ارائه می‌دهیم.

مثال ۳.۳. فرض کنیم $\mathcal{R}_۲ = \frac{(\mathbb{F}_{۱۶}+u\mathbb{F}_{۱۶})[x;\Theta]}{\langle x^۴-۱\rangle}$ و θ نگاشت فروبنیوس $\theta(\alpha) = \alpha^۲$ که در آن $\alpha \in \mathbb{F}_{۱۶}$. واضح است که $o(\theta) = ۴$. همچنین فرض کنیم δ ریشه‌ی پانزدهم اولیه‌ی واحد در $\mathbb{F}_{۱۶}$ باشد، یعنی $\mathbb{F}_{۱۶} = \{۰, \delta, \cdots, \delta^{۱۴}, \delta^{۱۵} = ۱\}$ و نگاشت $\psi : \mathbb{F}_{۱۶}^۴ R_۲^۴ \longrightarrow \mathbb{F}_{۱۶}^{۱۲}$ با ضابطه $\psi(d_۰, d_۱, d_۲, d_۳, r_۰, r_۱, r_۲, r_۳) = (d_۰, d_۱, d_۲, d_۳, \varphi(r_۰, r_۱, r_۲, r_۳))$ باشد که در آن $d_i \in \mathbb{F}_{p^m}$ و $r_i = a_i + ub_i \in R_۲$ و

$$\varphi : R_۲^۴ \longrightarrow \mathbb{F}_{p^m}^۸,$$
$$\varphi(a_۰ + ub_۰, a_۱ + ub_۱, a_۲ + ub_۲, a_۳ + ub_۳) = (b_۰, a_۰ + b_۰, b_۱, a_۱ + b_۱, b_۲, a_۲ + b_۲, b_۳, a_۳ + b_۳).$$

مدول‌های زیر را در نظر می‌گیریم:

$$C = \mathcal{R}_۲\big((\delta + (x-۱), (x-۱)^۲ + u\delta(x-۱))\big) = \mathcal{R}_۲\big(((۱+\delta)+x, (۱+u\delta)+u\delta x + x^۲)\big) \quad (۱).$$

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

$$\begin{bmatrix} ۱+\delta & ۱ & ۰ & ۰ & ۱+u\delta & u\delta & ۱ & ۰ \\ ۰ & (۱+\delta)^۲ & ۱ & ۰ & ۰ & ۱+u\delta^۲ & u\delta^۲ & ۱ \\ ۱+\delta & ۱ & \delta & ۱ & u\delta & u\delta & u(۱+\delta) & u(۱+\delta) \end{bmatrix},$$

و

$$\begin{bmatrix} ۱+\delta & ۱ & ۰ & ۰ & \delta & ۱+\delta & \delta & \delta & ۰ & ۱ & ۰ & ۰ \\ ۰ & (۱+\delta)^۲ & ۱ & ۰ & ۰ & ۰ & \delta^۲ & ۱+\delta^۲ & \delta^۲ & \delta^۲ & ۰ & ۱ \\ ۱+\delta & ۱ & \delta & ۱ & \delta & \delta & \delta & \delta & \delta+۱ & \delta+۱ & \delta+۱ & \delta+۱ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \end{bmatrix}.$$

لذا $\psi(C)$ یک کد بهینه با پارامترهای $[۱۲, ۵, ۴]$ روی $\mathbb{F}_{۱۶}$ است.

$$C=\mathcal{R}_۲\big((\delta,(x-۱)^۲+u\delta)\big)=\mathcal{R}_۲\big((\delta,(۱+u\delta)+x^۲)\big) \quad (۲).$$

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

$$\begin{bmatrix}
\delta & ۰ & ۰ & ۰ & ۱+u\delta & ۰ & ۱ & ۰ \\
۰ & \delta^۲ & ۰ & ۰ & ۰ & ۱+u\delta^۲ & ۰ & ۱ \\
\delta & ۰ & ۱+\delta & ۰ & u\delta & ۰ & u(۱+\delta) & ۰ \\
۰ & \delta^۲ & ۰ & (۱+\delta)^۲ & ۰ & u\delta^۲ & ۰ & u(۱+\delta)^۲
\end{bmatrix},$$

و

$$\begin{bmatrix}
\delta & ۰ & ۰ & ۰ & \delta & ۱+\delta & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ \\
۰ & \delta^۲ & ۰ & ۰ & ۰ & ۰ & \delta^۲ & ۱+\delta^۲ & ۰ & ۰ & ۰ & ۱ \\
\delta & ۰ & ۱+\delta & ۰ & \delta & \delta & ۰ & ۰ & ۱+\delta & ۱+\delta & ۰ & ۰ \\
۰ & \delta^۲ & ۰ & (۱+\delta)^۲ & ۰ & ۰ & \delta^۲ & \delta^۲ & ۰ & ۰ & (۱+\delta)^۲ & (۱+\delta)^۲ \\
۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ \\
۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱
\end{bmatrix}.$$

بنابراین $\psi(C)$ یک کد بهینه با پارامترهای $[۱۲,۶,۴]$ روی $\mathbb{F}_{۱۶}$ است.

مثال ۴.۳. فرض کنیم $\mathcal{R}_۲=\frac{(\mathbb{F}_{۲۷}+u\mathbb{F}_{۲۷})[x;\Theta]}{\langle x^۳-۱\rangle}$ و θ نگاشت فروبنیوس با ضابطه $\theta(\alpha)=\alpha^۳$. در این صورت $o(\theta)=۳$. همچنین فرض کنیم δ ریشه‌ی بیست و ششم اولیه‌ی واحد در $\mathbb{F}_{۲۷}$ باشد، یعنی $\mathbb{F}_{۲۷}=\{۰,\delta,\cdots,\delta^{۲۵},\delta^{۲۶}=۱\}$ و نگاشت $\psi:\mathbb{F}_{۲۷}^۳R_۲^۳\longrightarrow\mathbb{F}_{۲۷}^۹$ با ضابطه $\psi(d_۰,d_۱,d_۲,r_۰,r_۱,r_۲)=(d_۰,d_۱,d_۲,\varphi(r_۰,r_۱,r_۲))$ باشد که در آن $d_i\in\mathbb{F}_{p^m}$ و $r_i=a_i+ub_i\in R_۲$ و

$$\varphi:R_۲^۳\longrightarrow\mathbb{F}_{p^m}^۶,$$
$$\varphi(a_۰+ub_۰,a_۱+ub_۱,a_۲+ub_۲)=(b_۰,a_۰+b_۰,b_۱,a_۱+b_۱,b_۲,a_۲+b_۲).$$

به‌علاوه، $(x-۱)^۳=(x-\delta^۲)(x-\delta^{۱۸})(x-\delta^۶)$ یک تجزیه از $(x-۱)^۳$ در $\mathbb{F}_{۲۷}[x;\Theta]$ است. مدول‌های زیر را در نظر می‌گیریم:

$$C=\mathcal{R}_۲\big((۱,(x-\delta^۲)+u)\big)=\mathcal{R}_۲\big((۱,(۲\delta^۲+u)+x)\big) \quad (۱).$$

C و $\psi(C)$ به ترتیب دارای ماتریس مولد زیرند:

$$\begin{bmatrix}
۱ & ۰ & ۰ & ۲\delta^۲+u & ۱ & ۰ \\
۰ & ۱ & ۰ & ۰ & ۲(۱+\delta+\delta^۲)+u & ۱ \\
۱-\delta-\delta^۲ & ۱-\delta+\delta^۲ & ۱ & u(۱-\delta-\delta^۲) & u(۱-\delta+\delta^۲) & u
\end{bmatrix},$$

و

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1+2\delta^2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2(\delta+\delta^2) & 0 & 1 \\ 1-\delta-\delta^2 & 1-\delta+\delta^2 & 1 & 1-\delta-\delta^2 & 1-\delta-\delta^2 & 1-\delta+\delta^2 & 1-\delta+\delta^2 & 1 & 1 \\ 0 & 0 & 0 & 2\delta^2 & 2\delta^2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2(1+\delta+\delta^2) & 2(1+\delta+\delta^2) & 1 & 1 \end{bmatrix}.$$

لذا $\psi(C)$ یک کد بهینه با پارامترهای $[9, 5, 4]$ روی $\mathbb{F}_{27}$ است.

$$C = \mathcal{R}_2\big((1, (x-\delta^6)+u)\big) = \mathcal{R}_2\big((1, (2\delta^6+u)+x)\big) \quad (2)$$

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

$$\begin{bmatrix} 1 & 0 & 0 & (2-\delta-\delta^2)+u & 1 & 0 \\ 0 & 1 & 0 & 0 & 2(1-\delta+\delta^2)+u & 1 \\ 1+\delta-\delta^2 & \delta^2 & 1 & u(1+\delta-\delta^2) & u\delta^2 & u \end{bmatrix},$$

و

$$\begin{bmatrix} 1 & 0 & 0 & 1 & -\delta-\delta^2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & \delta-\delta^2 & 0 & 1 \\ 1+\delta-\delta^2 & \delta^2 & 1 & 1+\delta-\delta^2 & 1+\delta-\delta^2 & \delta^2 & \delta^2 & 1 & 1 \\ 0 & 0 & 0 & 2-\delta-\delta^2 & 2-\delta-\delta^2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2(1-\delta+\delta^2) & 2(1-\delta+\delta^2) & 1 & 1 \end{bmatrix}.$$

بنابراین $\psi(C)$ یک کد بهینه با پارامترهای $[9, 5, 4]$ روی $\mathbb{F}_{27}$ است.

۴ نتیجه گیری

فرض کنیم $R_2 = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ حلقه‌ی زنجیری و $\theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$ باشد. خودریختی $\Theta \in \mathrm{Aut}(R_2)$ را با ضابطه‌ی $\Theta(a+ub) = \theta(a) + u\theta(b)$ تعریف می‌کنیم. همچنین فرض کنیم $\mathcal{R}_1 = \frac{\mathbb{F}_{p^m}[x;\Theta]}{\langle x^{p^s}-1\rangle}$ و $\mathcal{R}_2 = \frac{R_2[x;\Theta]}{\langle x^{p^s}-1\rangle}$. زیرمجموعه‌ی $C \subseteq \mathcal{R}_1 \times \mathcal{R}_2$ را یک کد Θ- دوری اریب $\mathbb{F}_{p^m}R_2$-جمعی با طول $2p^s$ نامند، هرگاه C یک $R_2[x;\Theta]$- زیرمدول چپ از $\mathcal{R}_1 \times \mathcal{R}_2$ باشد. در این مقاله، ساختار جبری این دسته از کدها را بررسی و مولدهای آنها را مشخص کردیم. این کدها را برحسب چندجمله‌ای مولد آنها به ۸ دسته‌ی مجزا تقسیم کردیم. همچنین کدهای دوری $\mathbb{F}_{p^m}R_2$-جمعی از طول $2p^s$ به‌عنوان حالت خاص از این دسته از کدها به‌دست می‌آیند. این مطالعات را می‌توان با مشخص کردن دوگان کدهای دوری اریب $\mathbb{F}_{p^m}R_2$-جمعی از طول $2p^s$ و بررسی

کدهای خود دوگان از این نوع ادامه داد.

تشکر و قدردانی

نویسندگان مقاله از سردبیر مجله و همچنین از داوران محترم که زحمت داوری مقاله را قبول کرده و نظرات ارزشمندی در راستای بهبود مقاله پیشنهاد دادند قدردانی می‌کنند.

فهرست منابع

[1] Abualrub T., Siap I. and Aydin N., $\mathbb{Z}_2\mathbb{Z}_4$-*Additive cyclic code*, IEEE. Trans. Inf. Theory., 60(3) (2014), 1508-1514.

[2] Aydogdu I., Abualrub T., Siap I. and Aydin N., *On* $\mathbb{Z}_2\mathbb{Z}_2[u]$-*additive codes*, Int. J. Comput. Math., 92(9) (2015), 1806-1814.

[3] Borges J., Fernandez Cordoba C. and Ten Valls R., *Linear and cyclic codes over direct product of chain rings*, Math. Meth. Appl. Sci., (2017), 6519-6529.

[4] Boucher D., Geiselmann W. and Ulmer F., *Skew-cyclic codes*, Appl. Algebra Eng. Commun. Comput., 18 (2007), 379-389.

[5] Dinh H.Q., *Constacyclic codes of length* p^s *over* $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, J. Algebra., 324 (2010), 940-950.

[6] Jitman S., Ling S. and Udomkavanich P., *Skew constacyclic codes over finite chain ring*, Adv. Math. Commun., 6 (2012), 39-63.

[7] Mahmoudi S. and Samei K., *SR-Additive codes*, Bull. Korean Math. Soc., 56 (2019), 1235-1255.

[8] Mahmoodi H.R. and Sobhani R., *On some constacyclic codes over the ring* $\frac{\mathbb{F}_q[u]}{\langle u^4\rangle}$, Discrete Math., (2014), 3106-3122.

[9] McDonald B.R., *Finite rings with identity*, Marcel Dekker, New York, 1974.

$\mathbb{F}_{p^m}(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})$-Additive skew cyclic codes of length $2p^s$

Saeid Bagheri[1], **Roghayeh Mohammadi Hesari**[1], **Hamed Rezaei**[1], **Rashid Rezaei**[1], **Karim Samei**[2] [†],

[(1)] Department of Mathematics, Faculty of Mathematical Sciences and Statistics, Malayer University, Malayer, Iran

[(2)] Department of Mathematics, Faculty of Basic Science, Bu-Ali Sina University, Hamedan, Iran

Communicated by: M. Namdari

Received: 2021/2/19 Accepted: 2021/10/20

Abstract: Let p be a prime number and R_2 be the ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, where $u^2=0$. In this paper, we study the algebraic structure of $\mathbb{F}_{p^m}R_2$-additive skew cyclic codes of length $2p^s$ and we determine a set of generator polynomials for this family of codes. These codes will be classified into eight distinct types of submodules. Finally, using a Gray map, we present some examples of $\mathbb{F}_{p^m}R_2$-additive skew cyclic codes of length $2p^s$.

Keywords: Additive skew cyclic code, Chain ring, Gray map.

Mathematics Subject Classification (2010): 94 B15, 16S36.

[†] **Corresponding author:** samei@ipm.ir