مجله مدل‌سازی پیشرفته ریاضی
سال ۱۴۰۲، دوره ۱۳، شماره ۱، ص ۱۰۶-۱۱۵

شاپا چاپی: ۲۲۵۱-۸۰۸۸
DOI: 10.22055/JAMM.2023.43717.2161

یک رده از کدهای دوادیک پاددوری روی حلقه $\mathbb{F}_q + v\mathbb{F}_q$ و توسیع آن‌ها

محمد گلپریان [۱]، رشید رضائی [۱] ×، کریم سامعی [۲]

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

دبیر مسئول: مهرداد نامداری

تاریخ دریافت: ۱۴۰۲/۲/۲۰ تاریخ پذیرش: ۱۴۰۲/۳/۱۶

چکیده: بلکفورد در سال ۲۰۰۸ [۱] مفهوم کدهای دوادیک پاددوری را روی میدان $\mathbb{F}_q$ معرفی کرد و تمام کدهای پایادوری خوددوگان روی میدان $\mathbb{F}_q$ را رده‌بندی کرد. در این مقاله کدهای دوادیک پاددوری را روی حلقه $\mathbb{F}_q + v\mathbb{F}_q$ معرفی می‌کنیم و با استفاده از نگاشت گری روی این کدها، کدهای خوددوگان و خودمتعامد روی میدان $\mathbb{F}_q$ به‌دست می‌آوریم. هم‌چنین توسیع‌هایی ازکدهای دوادیک پاددوری را روی حلقه $\mathbb{F}_q + v\mathbb{F}_q$ معرفی کرده و خواص آن‌ها را بررسی می‌کنیم. در پایان مثال‌هایی از کدهای دوادیک پاددوری روی این حلقه و کدهای خودمتعامد و خوددوگان روی میدان $\mathbb{F}_q$ ارائه می‌دهیم.

واژه‌های کلیدی: کد پاددوری،کد خوددوگان،کد خودمتعامد.

رده‌بندی ریاضی: 94B05; 11T71

۱ مقدمه

بررسی کدهای خطی روی حلقه‌های متناهی از چند دهه پیش مورد توجه محققین قرار گرفته است، اما علاقه به مطالعه این کدها پس از آن بیش‌تر شد که هامونز و هم‌کارانش در [۴] موفق شدند برخی از کدهای غیرخطی دودویی معروف را توسط تصویر نگاشت گری کدهای خطی روی $\mathbb{Z}_4$ به‌دست آورند. تاکنون تحقیقات زیادی روی کدهای دوری، پایا دوری و کدهای باقی‌مانده درجه دوم، روی برخی از حلقه‌های متناهی انجام شده است. کدهای دوادیک برای اولین بار توسط لئون و هم‌کارانش در [۷] معرفی شد. این کدها یک کلاس شناخته‌شده از کدهای دوری‌اند که به ساخت کدهای خوددوگان منجر می‌شوند. از جمله حالت‌های خاص کدهای دوادیک می‌توان به کدهای باقی‌مانده درجه دوم اشاره نمود. جالب این‌که کدهای گولای و هکسا را می‌توان توسط کدهای باقی‌مانده درجه‌دوم به‌دست آورد. در سال ۲۰۰۸ میلادی مفهوم کدهای دوادیک پاددوری روی میدان $\mathbb{F}_q$ توسط بلکفورد تعریف و مورد مطالعه قرار گرفت [۱]. وی هم‌چنین کدهای دوادیک پایادوری را روی $\mathbb{F}_q$ مطالعه نمود که منجر به یافتن کدهای پایادوری ایزودوگان شد [۲]. در این مقاله کدهای دوادیک پاددوری روی حلقه

×نویسنده مسئول مقاله
رایانامه: ras_razaei@yahoo.com ؛r.rezaei@malayeru.ac.ir

$R = \mathbb{F}_q + v\mathbb{F}_q$ که در آن $v^2 = v$، تعریف و مورد مطالعه قرار می‌گیرد. در بخش ۲ تعاریف و مفاهیم مقدماتی مورد نیاز معرفی می‌شود. در بخش ۳ کدهای دوادیک پاددوری روی حلقه $R = \mathbb{F}_q + v\mathbb{F}_q$ تعریف و مورد مطالعه قرار می‌گیرد. خصوصیات کدهای دوادیک پاددوری توسعه‌یافته در بخش ۴ بررسی می‌شود. در بخش ۵ با استفاده از تصویر نگاشت گری کدها روی R، مثال‌هایی از کدهای خوددوگان و خودمتعامد ارائه می‌شود.

۲ تعاریف و مقدمات

در این بخش مفاهیم، تعاریف و قضایای مورد استفاده در این مقاله را به‌اختصار بیان می‌کنیم.
فرض کنیم q توانی از یک عدد اول فرد و $\mathbb{F}_q$ میدانی متناهی با q عنصر باشد. حلقه

$$R = \mathbb{F}_q + v\mathbb{F}_q = \{a + vb : a, b \in \mathbb{F}_q\},$$

با شرط $v^2 = v$ یک حلقه جابه‌جایی از مرتبه q^2 و مشخصه q است. حلقه $\mathbb{F}_q + v\mathbb{F}_q$ با حلقه $\mathbb{F}_q \times \mathbb{F}_q$ یکریخت است. این حلقه دارای دو ایده‌آل ماکسیمال به‌صورت زیر است [۹]:

$$\langle v \rangle = \{av : a \in \mathbb{F}_q\}\ ,\ \langle 1 - v \rangle = \{b - bv : b \in \mathbb{F}_q\}.$$

فرض کنیم

$$R_{q,n} := \frac{(\mathbb{F}_q + v\mathbb{F}_q)[x]}{\langle x^n + 1 \rangle}.$$

برای راحتی کار، چندجمله‌ای $f(x)$ روی حلقه $R_{q,n}$ را با f نمایش می‌دهیم. عنصر $e(x)$ از حلقه $R_{q,n}$ را خودتوان گوییم هرگاه $e^2(x) = e(x)$. مشابه لم ۱.۲ در [۶] می‌توان نشان داد مجموعه همه عناصر خودتوان $R_{q,n}$ به‌صورت زیرند:

$$\left\{ (1 - v)f + vg : f \text{ و } g \text{ عناصر خودتوان در } \frac{\mathbb{F}_q[x]}{\langle x^n + 1 \rangle} \text{ اند} \right\}.$$

گزاره **۱.۲**. مشابه لم ۲.۲ در [۶] فرض کنیم f و g عناصر خودتوان $\frac{\mathbb{F}_q[x]}{\langle x^n + 1 \rangle}$، $C_1 = \langle f \rangle$ و $C_2 = \langle g \rangle$ کدهای دوری روی حلقه جابه‌جایی یکدار R باشند. در این‌صورت $C_1 \cap C_2$ و $C_1 + C_2$ به‌ترتیب دارای مولدهای خودتوان fg و $f + g - fg$اند.

یک کد با طول n روی R یک زیرمجموعه غیر تهی از R^n است. یک کد روی R را خطی گویند هرگاه یک R-زیرمدول از R^n باشد. فرض کنیم C یک کد با طول n روی R و $P(C)$ چند جمله‌ای متناظر آن باشد. به‌عبارت دیگر

$$P(C) = \left\{ \sum_{i=0}^{n-1} c_i x^i : \ (c_0, c_1, ..., c_{n-1}) \in C \right\}.$$

نگاشت $\gamma : R^n \longrightarrow R^n$ را به‌صورت زیر در نظر بگیریم:

$$\gamma(c_0, c_1, ..., c_{n-1}) = (-c_{n-1}, c_0, ..., c_{n-2}).$$

در این‌صورت C را پاددوری گوییم هرگاه $\gamma(C) = C$. یک کد با طول n روی R پاددوری است اگر و تنها اگر $P(C)$ ایده‌آلی از حلقه خارج قسمتی $R_{q,n}$ باشد [۵].
فرض کنیم $x, y \in R^n$ به‌صورت زیر باشند:

$$x = (x_0, x_1, ..., x_{n-1}), \qquad y = (y_0, y_1, ..., y_{n-1}).$$

در این‌صورت ضرب داخلی اقلیدسی x و y روی R^n به‌صورت

$$x \cdot y = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1},$$

تعریف می‌شود که در آن عملیات روی R انجام می‌گیرد. کد دوگان اقلیدسی C به صورت زیر تعریف می‌شود:

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

اگر $C \subseteq C^\perp$، آن‌گاه کد C را خودمتعامد اقلیدسی و اگر $C = C^\perp$، آن را خوددوگان اقلیدسی می‌نامیم.

گزاره **۲.۲**. [۳] (قضیه باقی‌مانده چینی) فرض کنیم R یک حلقه جابه‌جایی متناهی با ایده‌آل‌های ماکسیمال $m_s, ..., m_۲, m_۱$ باشد به‌طوری‌که درجه‌ی پوچ‌توانی هر m_i برابر e_i است. در این‌صورت نگاشت زیر، یک یکریختی حلقه‌ای خواهد بود:

$$\psi : R \to \prod_{i=۱}^{s} \frac{R}{m_i^{e_i}},$$

$$\psi(x) = (x + m_۱^{e_۱}, ..., x + m_s^{e_s}).$$

فرض کنیم برای $۱ \leq i \leq s$، R_i نشان‌دهنده حلقه $\frac{R}{m_i^{e_i}}$ باشد. بنابر قضیه فوق داریم:

$$R \cong R_۱ \times R_۲ \times \cdots \times R_s.$$

وارون یکریختی ψ را با نماد CRT مشخص می‌کنیم. بنابراین

$$CRT : R_۱ \times R_۲ \times \cdots \times R_s \to R.$$

فرض کنیم C_i یک کد روی R_i و $C = CRT(C_۱, C_۲, ..., C_s)$ کدی روی R باشد که توسط یکریختی فوق حاصل شده است. در این‌صورت هر کد C روی R تصویر تعدادی مجموعه کدهای $C_۱$، $C_۲$، ... و C_s است.

گزاره **۳.۲**. [۳] فرض کنیم $R = CRT(R_۱, R_۲, ..., R_s)$ یک حلقه جابه‌جایی متناهی و $C = CRT(C_۱, C_۲, ..., C_s)$ یک کد روی R باشد. در این‌صورت $C^{\perp} = CRT(C_۱^{\perp}, C_۲^{\perp}, ..., C_s^{\perp})$.

گزاره **۴.۲**. [۳] فرض کنیم R یک حلقه جابه‌جایی متناهی باشد که طبق قضیه باقی‌مانده چینی با $R_۱ \times R_۲ \times \cdots \times R_s$ یکریخت است. هم‌چنین C_i یک کد روی R_i و $C = CRT(C_۱, C_۲, ..., C_s)$ باشد. در این‌صورت C یک کد خوددوگان روی R است اگر و تنها اگر برای هر i، C_i کد خوددوگان روی R_i باشد.

نگاشت گری در [۱۰] به‌صورت زیر تعریف می‌شود:

$$\Phi : \mathbb{F}_q + v\mathbb{F}_q \to \mathbb{F}_q^{۲}$$
$$a + bv \to (-b, ۲a + b).$$

وزن لی هر عضو در $R = \mathbb{F}_q + v\mathbb{F}_q$ به‌عنوان وزن همینگ تصویر نگاشت گری آن تعریف می‌شود. این نگاشت را می‌توان روی R^n به‌صورت زیر توسیع داد:

$$\Phi : R^n \to \mathbb{F}_q^{۲n}$$
$$(c_۰, c_۱, ..., c_{n-۱}) \mapsto (-b_۰, -b_۱, ..., -b_{n-۱}, ۲a_۰ + b_۰, ۲a_۱ + b_۱, ..., ۲a_{n-۱} + b_{n-۱})$$

که در آن $c_i = a_i + b_i v$ $(i = ۰, ..., n - ۱)$.

گزاره **۵.۲**. [۱۰] نگاشت گری Φ یک نگاشت حافظ فاصله از R^n (فاصله لی) به $\mathbb{F}_q^{۲n}$ (فاصله همینگ) و $\mathbb{F}_q$-خطی است.

۳ کدهای دوادیک پاددوری روی $\mathbb{F}_q + v\mathbb{F}_q$

فرض کنیم n' یک عدد صحیح فرد، $n = ۲n'$ و q توانی از یک عدد اول فرد باشد که نسبت به n اول است. علاوه بر این، فرض کنیم δ ریشه $۲n$ام اولیه واحد در میدان توسیعی $\mathbb{F}_q$ باشد. به‌وضوح $\delta^{۲i+۱}$ همه ریشه‌های $x^n + ۱$ اند که در آن $۰ \leq i \leq n - ۱$. فرض کنیم $O_{۲n}$ مجموعهٔ اعداد صحیح فرد از ۱ تا $۲n + ۱$ باشد. مجموعه تعریف کد پاددوری $C = \langle g(x) \rangle$ با طول n مجموعه $T = \{i \in O_{۲n} : \text{است } C \text{ ریشه } \delta^i\}$ است که اجتماع هم‌رده‌های q-دایره‌بری به پیمانه $۲n$ است و $|C| = n - |T|$.

تعریف **۱.۳**. چندجمله‌ای $c(x) = c_۰ + c_۱x + c_۲x^۲ + \cdots + c_{n-۱}x^{n-۱}$ در $R_{q,n}$ را شبه‌زوج نامیم هرگاه $x^۲ + ۱$ آن را بشمارد. به‌عبارت دیگر $c(\delta^{\frac{n}{۲}})$ و $c(\delta^{\frac{۳n}{۲}})$ برابر صفر باشند. یک کد پاددوری را شبه‌زوج نامیم هرگاه کدواژه‌های آن شبه‌زوج باشند. یک کد را شبه‌فرد نامیم هرگاه شبه‌زوج نباشد.

تعریف **۲.۳**. فرض کنیم n یک عدد صحیح نامنفی و $۱ \leq s \leq ۲n-۱$ به‌طوری که $gcd(s, ۲n) = ۱$. نگاشت ضربی μ_s را روی $R_{q,n}$ به‌صورت زیر تعریف می‌کنیم:

$$\mu_s : R_{q,n} \to R_{q,n}$$

$$\mu_s(a(x)) = a(x^s) \pmod{(x^n+۱)},$$

که در آن μ_s یک خودریختی از $R_{q,n}$ است. هم‌چنین μ_s یک نگاشت به‌صورت زیر القا می‌کند:

$$\mu'_s : O_{۲n} \to O_{۲n}$$

$$\mu'_s(i) = si \pmod{۲n}.$$

تعریف **۳.۳**. یک q–شکافت از n یک نگاشت ضربی μ_s از n است که یک افراز از $O_{۲n}$ را با شرایط زیر القاء می‌کند:

(۱) $O_{۲n} = A \cup B \cup X$.

(۲) A، B و X اجتماعی از هم‌مجموعه‌های q– دایره‌بری به پیمانه $۲n$اند.

(۳) $\mu'_s(B) = A$ ، $\mu'_s(A) = B$ و $\mu'_s(X) = X$.

- یک شکافت از نوع I نامیده می‌شود هرگاه $X = \emptyset$.
- یک شکافت از نوع II نامیده می‌شود هرگاه $X = \left\{ \frac{n}{۲}, \frac{۳n}{۲} \right\}$.

کد پاددوری C از طول n را دوادیک نامند، هرگاه یک q–شکافت وجود داشته باشد و مجموعه تعریف آن‌ها یکی از مجموعه‌هایA، B، $A \cup X$ و $B \cup X$ باشد.
اگر s شکافتی از نوع II ایجاد کند، آن‌گاه برای $A(x), B(x) \in R[x]$ داریم:

$$x^n + ۱ = A(x)B(x)(x^۲ + ۱),$$

به‌طوری‌که

$$\mu_s(\langle A(x) \rangle) = \langle B(x) \rangle \ , \ \mu_s(\langle B(x) \rangle) = \langle A(x) \rangle.$$

هم‌چنین اگر δ^i یک ریشه از $A(x)$ باشد، آن‌گاه δ^{si} یک ریشه از$B(x)$ است و به‌عکس [۱].
بنابر نتیجه ۱۰ در [۱]، اگر $q = ۳ \pmod{۴}$، آن‌گاه کدهای دوادیک پاددوری با طول n روی $\mathbb{F}_q$ وجود دارد. در واقع

$$x^n + ۱ = A(x)B(x)(x^۲ + ۱)$$

$$\begin{cases} C_۱ = \langle e_۱(x) \rangle = \langle (x^۲+۱)A(x) \rangle, \\ C_۲ = \langle e_۲(x) \rangle = \langle (x^۲+۱)B(x) \rangle, \\ D_۱ = \langle ۱ - e_۲(x) \rangle = \langle A(x) \rangle, \\ D_۲ = \langle ۱ - e_۱(x) \rangle = \langle B(x) \rangle, \end{cases}$$

که $C_۱$، $C_۲$، $D_۱$ و $D_۲$ کدهای دوادیک پاددوری از طول n روی $\mathbb{F}_q$ اند و $e_۱(x)$ و $e_۲(x)$ خودتوان‌اند. برای راحتی کار، از این به بعد $e_i(x)$ را با e_i نشان می‌دهیم.

گزاره **۴.۳**. [۱] فرض کنیم $C_۱$ و $C_۲$ یک جفت کد دوادیک پاددوری شبه‌زوج از نوع II و $D_۱$ و $D_۲$ یک جفت کد دوادیک پاددوری شبه‌فرد متناظر با آن‌ها روی میدان $\mathbb{F}_q$ باشند. اگر $s = ۲n - ۱$، آن‌گاه $C_۱^\perp = D_۱$ و$C_۲^\perp = D_۲$.

حال کدهای دوادیک پاددوری را روی حلقه $R = \mathbb{F}_q + v\mathbb{F}_q$ تعریف می‌کنیم. قرار می‌دهیم:

$$\begin{cases} \mathcal{C}_1 = \langle (1-v)e_1 + ve_2 \rangle, \\ \mathcal{C}_2 = \langle (1-v)e_2 + ve_1 \rangle, \\ \mathcal{D}_1 = \langle (1-v)(1-e_2) + v(1-e_1) \rangle, \\ \mathcal{D}_2 = \langle (1-v)(1-e_1) + v(1-e_2) \rangle. \end{cases}$$

$\mathcal{C}_1$ و $\mathcal{C}_2$ یک جفت کد دوادیک پادوری شبه‌زوج و $\mathcal{D}_1$ و $\mathcal{D}_2$ یک جفت کد دوادیک پاددوری شبه‌فرد از طول n روی $\mathbb{F}_q + v\mathbb{F}_q$ نامیده می‌شوند.

فرض کنیم $J(x) = A(x)B(x)$. بنابراین

$$x^n + 1 = A(x)B(x)(x^2 + 1) = (x^2 + 1)J(x).$$

لذا داریم:

$$x^n + 1 = x^{2n'} + 1 = (x^2)^{n'} + 1 = \Big(x^2 + 1\Big)\Big(1 - x^2 + x^4 - \cdots + x^{2(n'-1)}\Big).$$

به‌وضوح $J(x) = 1 - x^2 + x^4 - \cdots + x^{2(n'-1)}$ و $J^2(x) = \frac{n}{2}J(x)$.

قرار می‌دهیم $\overline{J}(x) = \frac{2}{n}J(x)$؛ بدیهی است که $\overline{J}(x)$ خودتوان است.

اکنون به بررسی ویژگی‌های این کدها می‌پردازیم.

گزاره **۵.۳**. فرض کنیم $\mathcal{C}_1$ و $\mathcal{C}_2$ یک جفت کد دوادیک پاددوری شبه‌زوج از نوع II، و $\mathcal{D}_1$ و $\mathcal{D}_2$ یک جفت کد دوادیک پاددوری شبه‌فرد متناظر با آن‌ها روی میدان $\mathbb{F}_q + v\mathbb{F}_q$ باشد. برای این کدها گزاره‌های زیر برقرارند:

۱. $\mu_s(\mathcal{C}_1) = \mathcal{C}_2, \quad \mu_s(\mathcal{C}_2) = \mathcal{C}_1$.

۲. $\mu_s(\mathcal{D}_1) = \mathcal{D}_2, \quad \mu_s(\mathcal{D}_2) = \mathcal{D}_1$.

۳. $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}, \quad \mathcal{C}_1 + \mathcal{C}_2 = \langle e_1 + e_2 \rangle$.

۴. $\mathcal{D}_1 \oplus \mathcal{C}_2 = \mathcal{D}_2 \oplus \mathcal{C}_1 = (\mathbb{F}_q + v\mathbb{F}_q)^n$.

۵. $\mathcal{D}_1 \cap \mathcal{D}_2 = \langle \overline{J}(x) \rangle = \langle 1 - e_1 - e_2 \rangle, \quad \mathcal{D}_1 + \mathcal{D}_2 = R_{q,n}$.

۶. $\mathcal{D}_1 = \mathcal{C}_1 + \langle \overline{J}(x) \rangle, \quad \mathcal{D}_2 = \mathcal{C}_2 + \langle \overline{J}(x) \rangle$.

۷. اگر $s = 2n - 1$ باشد، آن‌گاه $\mathcal{D}_1^{\perp} = \mathcal{C}_1, \ \mathcal{D}_2^{\perp} = \mathcal{C}_2$.

۸. C_1 و C_2 خودمتعامداند.

اثبات. ۱. بنابر تعریف داریم:

$$\mu_s(\mathcal{C}_1) = \mu_s(\langle (1-v)e_1 + ve_2 \rangle) = \langle (1-v)e_2 + ve_1 \rangle = \mathcal{C}_2.$$

به‌طور مشابه

$$\mu_s(\mathcal{C}_2) = \mu_s(\langle (1-v)e_2 + ve_1 \rangle) = \langle (1-v)e_1 + ve_2 \rangle = \mathcal{C}_1.$$

۲.

$$\begin{aligned} \mu_s(\mathcal{D}_1) &= \mu_s(\langle (1-v)(1-e_2) + v(1-e_1) \rangle) \\ &= \langle (1-v)(1-e_1) + v(1-e_2) \rangle = \mathcal{D}_2. \end{aligned}$$

به‌طور مشابه

$$\begin{aligned} \mu_s(\mathcal{D}_2) &= \mu_s(\langle (1-v)(1-e_1) + v(1-e_2) \rangle) \\ &= \langle (1-v)(1-e_2) + v(1-e_1) \rangle = \mathcal{D}_1. \end{aligned}$$

۳. $\mathcal{C}_1 \cap \mathcal{C}_2$ دارای مولد خودتوانی به‌صورت زیر است:

$$[(1-v)e_1 + ve_2)][(1-v)e_2 + ve_1] = [e_1 - ve_1 + ve_2][e_2 - ve_2ve_1] = 0.$$

$\mathcal{C}_1 + \mathcal{C}_2$ دارای مولد خودتوانی به‌صورت زیر است:

$$\begin{aligned}[(1-v)e_1 + ve_2)] + [(1-v)e_2 + ve_1] \\ - [(1-v)e_1 + ve_2][(1-v)e_2 + ve_1] \\ = e_1 + e_2.\end{aligned}$$

۴. $\mathcal{D}_1 + \mathcal{C}_2$ دارای مولد خودتوانی به‌صورت زیر است:

$$\begin{aligned}[(1-v)(1-e_2) + v(1-e_1)] + [(1-v)e_2 + ve_1] \\ - [(1-v)(1-e_2) + v)(1-e_1)][(1-v)e_2 + ve_1] \\ = 1.\end{aligned}$$

بنابراین $\mathcal{D}_1 \oplus \mathcal{C}_2 = (\mathbb{F}_q + v\mathbb{F}_q)^n$. به‌روش مشابه، تساوی برای $\mathcal{C}_1 \oplus \mathcal{D}_2$ اثبات می‌شود.

۵. $\mathcal{D}_1 \cap \mathcal{D}_2$ دارای مولد خودتوانی به‌صورت زیر است:

$$\begin{aligned}[(1-v)(1-e_2) + v(1-e_1)][(1-v)(1-e_1) + v(1-e_2)] \\ = 1 - e_1 - e_2 = \overline{J}(x).\end{aligned}$$

$\mathcal{D}_1 + \mathcal{D}_2$ دارای مولد خودتوانی به‌صورت زیر است:

$$\begin{aligned}[(1-v)(1-e_2) + v(1-e_1)][(1-v)(1-e_1) + v(1-e_2)] \\ - [(1-v)(1-e_2) + v(1-e_1)][(1-v)(1-e_1) + v(1-e_1)] \\ = [1 - e_2 + ve_2 - v_1] + [1 - e_1 + ve_1 - ve_2] - [1 - e_1 - e_2] \\ = 1.\end{aligned}$$

بنابراین $\mathcal{D}_1 + \mathcal{D}_2 = R_{q,n}$.

۶. $\mathcal{C}_1 + \langle \overline{J}(x) \rangle$ دارای مولد خودتوانی به‌صورت زیر است:

$$\begin{aligned}[(1-v)e_1 + ve_2)][1 - e_1 - e_2] - [(1-v)e_1 + ve_2][1 - e_1 - e_2] \\ = 1 - ve_1 + ve_2 - e_2 \\ = (1-v)(1-e_2) + v(1-e_1).\end{aligned}$$

به‌روش مشابه ثابت می‌شود که $\mathcal{D}_2 = \mathcal{C}_2 + \langle \overline{J}(x) \rangle$.

۷. با استفاده از گزاره‌های ۲.۲ و ۳.۲ داریم:

$$\mathcal{D}_1^{\perp} = CRT(D_2^{\perp}, D_1^{\perp}) = CRT(C_2, C_1) = \mathcal{C}_1.$$

به‌روش مشابه ثابت می‌شود که $\mathcal{D}_2^{\perp} = \mathcal{C}_2$.

۸. از (۶) و (۷) نتیجه می‌شود $\mathcal{C}_1 \subset \mathcal{D}_1 \subset \mathcal{C}_1^{\perp}$. بنابراین $\mathcal{C}_1$ خودمتعامد است. به‌روش مشابه ثابت می‌شود که $\mathcal{C}_2$ نیز خودمتعامد است.

□

۴ توسیع کدهای پاددوری روی $\mathbb{F}_q + v\mathbb{F}_q$

کدهای خوددوگان از برخی طول‌ها وجود دارند اما این کدها لزوماً پاددوری نیستند و می‌توان با توسیع کدهای پاددوری به کدهای خوددوگان جدیدی برسیم. برای یک کد داده‌شده روی میدان $\mathbb{F}_q$ می‌توان توسیع‌های مختلفی تعریف کرد. یکی از این توسیع‌ها به‌صورت زیر تعریف می‌شود (مرجع [۱] را ببینید).

فرض کنیم n' یک عدد صحیح فرد، $n = ۲n'$ و q توانی از یک عدد اول فرد باشد که نسبت به n اول است و $-\frac{۲}{n}$ باقی‌مانده درجه دوم از عدد اول q باشد. در این‌صورت $\gamma \in \mathbb{F}_q^*$ وجود دارد به‌طوری‌که $\gamma^۲ n + ۲ = ۰$. عنصر $a = (a_۰, ..., a_{n-۱}) \in \mathbb{F}_q^n$ را در نظر می‌گیریم. $\hat{a}$ را به‌صورت $\hat{a} = (a_۰, ..., a_{n-۱}, a_\infty, a_*) \in \mathbb{F}_q^{n+۲}$ تعریف می‌کنیم که در آن

$$a_\infty = \gamma \sum_{i=۰}^{\frac{n-۱}{۲}} (-۱)^i a_{۲i} \ , \ a_* = \gamma \sum_{i=۰}^{\frac{n-۱}{۲}} (-۱)^i a_{۲i+۱}.$$

اگر C یک مجموعه از بردارهایی از طول n باشد، آن‌گاه $\hat{C}$ را به‌صورت مجموعه $\{\hat{a} : a \in C\}$ تعریف و آن را توسیع پاددوری C می‌نامیم. (توجه شود که C و $\hat{C}$ دارای بعد یکسانی‌اند).

حال اگر $C = CRT(C_۱, C_۲)$ آن‌گاه $\hat{C} = CRT(\hat{C}_۱, \hat{C}_۲)$ را تعریف کرده و آن را توسیع کد پاددوری می‌نامیم.

اکنون ویژگی‌های توسیع کدهای پاددوری را در گزاره زیر بیان می‌کنیم.

گزاره **۱.۴**. فرض کنیم q عددی اول باشد به‌طوری‌که برای $\gamma \in \mathbb{F}_q^*$ داشته باشیم $\gamma^۲ = -\frac{۲}{n}$. هم‌چنین فرض کنیم $\mathcal{D}_۱$ و $\mathcal{D}_۲$ کدهای دوادیک پاددوری شبه‌فرد با نگاشت ضربی μ_s از نوع II است.

۱. اگر $s = ۲n - ۱$، آن‌گاه $\hat{\mathcal{D}}_۱$ و $\hat{\mathcal{D}}_۲$ خوددوگان‌اند.

۲. اگر $\mu_{-۱}(\mathcal{D}_۱) = \mathcal{D}_۲$ و $\mu_{-۱}(\mathcal{D}_۲) = \mathcal{D}_۱$، آن‌گاه $\hat{\mathcal{D}}_۱^\perp = \hat{\mathcal{D}}_۲$ و $\hat{\mathcal{D}}_۲^\perp = \hat{\mathcal{D}}_۱$.

اثبات. ۱. فرض کنیم $\hat{\mathcal{D}}_۱ = CRT(\hat{D}_۲, \hat{D}_۱)$. در این‌صورت

$$\hat{\mathcal{D}}_۱^\perp = CRT(\hat{D}_۲^\perp, \hat{D}_۱^\perp) = CRT(\hat{D}_۲, \hat{D}_۱) = \hat{\mathcal{D}}_۱.$$

به‌روش مشابه، تساوی $\hat{\mathcal{D}}_۲^\perp = \hat{\mathcal{D}}_۲$ اثبات می‌شود.

۲. فرض کنیم $\hat{\mathcal{D}}_۱ = CRT(\hat{D}_۲, \hat{D}_۱)$. در این‌صورت

$$\hat{\mathcal{D}}_۱^\perp = CRT(\hat{D}_۲^\perp, \hat{D}_۱^\perp) = CRT(\hat{D}_۱, \hat{D}_۲) = \hat{\mathcal{D}}_۲.$$

به‌روش مشابه، تساوی $\hat{\mathcal{D}}_۲^\perp = \hat{\mathcal{D}}_۱$ اثبات می‌شود.

□

۵ مثال‌ها

در این بخش چند مثال از کدهای دوادیک پاددوری روی حلقه $\mathbb{F}_q + v\mathbb{F}_q$ را به‌دست می‌آوریم. با استفاده از تصویر نگاشت گری این کدها، مثال‌هایی از کدهای خوددوگان و خودمتعامد روی میدان $\mathbb{F}_q$ ارائه می‌دهیم.

مثال **۱.۵**. فرض کنیم $q = ۱۱$ و $\gamma = ۵$. داریم:

$$x^{۱۴} + ۱ = (x^۶ + ۴x^۴ + ۶x^۲ + ۱)(x^۶ + ۶x^۴ + ۴x^۲ + ۱)(x^۲ + ۱)$$

و

$$A(x) = x^۶ + ۴x^۴ + ۶x^۲ + ۱ \ , \ B(x) = x^۶ + ۶x^۴ + ۴x^۲ + ۱.$$

در این‌صورت

$$\begin{aligned}\mathcal{C}_۱ &= \langle (۱-v)(x^۶+۴x^۴+۶x^۲+۱)(x^۲+۱) \\ &\quad + v(x^۶+۶x^۴+۴x^۲+۱)(x^۲+۱)\rangle \\ &= \langle x^۸+(۵+۲v)x^۶+۱۰x^۴+(۷-۲v)x^۲+۱\rangle,\end{aligned}$$

که تصویر نگاشت گری آن یک کد خودمتعامد با پارامترهای $[۲۸, ۱۲, ۷]_{۱۱}$ است.

مثال **۲.۵**. فرض کنیم $q = ۳$ و $\gamma = ۱$. داریم:

$$x^{۱۰}+۱ = (x^۴+x^۳+۲x+۱)(x^۴+۲x^۳+x+۱)(x^۲+۱)$$

و

$$A(x) = x^۴+x^۳+۲x+۱ \ , \ B(x) = x^۴+۲x^۳+x+۱.$$

در این‌صورت

$$\begin{aligned}\mathcal{C}_۱ &= \langle (۱-v)(x^۴+x^۳+۲x+۱)(x^۲+۱) \\ &\quad + v(x^۴+۲x^۳+x+۱)(x^۲+۱)\rangle \\ &= \langle x^۶+(۲-v)x^۵+x^۴+x^۲+(۱+v)x+۱\rangle,\end{aligned}$$

که تصویر نگاشت گری آن یک کد خودمتعامد با پارامترهای $[۲۰, ۸, ۶]_۳$ است.

مثال **۳.۵**. فرض کنیم $q = ۷$ و $\gamma = ۲$. داریم:

$$x^{۱۰}+۱ = (x^۴+۳x^۳+۴x^۲+۴x+۱)(x^۴+۴x^۳+۴x^۲+۳x+۱)(x^۲+۱)$$

و

$$A(x) = x^۴+۳x^۳+۴x^۲+۴x+۱ \ , \ B(x) = x^۴+۴x^۳+۴x^۲+۳x+۱.$$

در این‌صورت

$$\begin{aligned}\mathcal{C}_۱ &= \langle (۱-v)(x^۴+۳x^۳+۴x^۲+۴x+۱)(x^۲+۱) \\ &\quad + v(x^۴+۴x^۳+۴x^۲+۳x+۱)(x^۲+۱)\rangle \\ &= \langle x^۶+(۳+v)x^۵+۵x^۴+۷x^۳+۵x^۲+(۵-v)x+۱\rangle,\end{aligned}$$

که تصویر نگاشت گری آن یک کد خودمتعامد با پارامترهای $[۲۰, ۸, ۴]_۷$ است.

مثال **۴.۵**. فرض کنیم $q = ۷$ و $\gamma = ۳$. داریم:

$$x^۶+۱ = (x^۲+۲)(x^۲+۴)(x^۲+۱)$$

و

$$A(x) = x^۲+۲ \ , \ B(x) = x^۲+۴.$$

در این‌صورت

$$\begin{aligned}\mathcal{D}_۱ &= \langle (۱-v)(x^۲+۲)+v(x^۲+۴)\rangle \\ &= \langle x^۲+(۲+۲v)\rangle,\end{aligned}$$

و $\hat{\mathcal{D}}_۱ = \{(d|d_\infty, d_*) : d \in \mathcal{D}_۱\}$، از این‌رو تصویر نگاشت گری $\hat{\mathcal{D}}_۱$ یک کد خوددوگان با پارامترهای $[۱۶, ۸, ۴]_۷$ است.

۶ نتیجه‌گیری

در این مقاله، کدهای دوادیک پاددوری روی حلقه $\mathbb{F}_q + \nu\mathbb{F}_q$ با مولدهای خودتوان ساخته شده است. ویژگی این کدها مشابه کدهای دوادیک‌اند و بیش‌تر قضایا و نتایج روی کدهای دوادیک قابل تعمیم برای کدهای دوادیک پاددوری‌اند. مهم آن است که طول کدهای دوادیک عددی اول است ولی طول کدهای دوادیک پاددوری دو برابر یک عدد فرد است. کدهای خوددوگان و خودمتعامد با پارامترهای مناسب به‌عنوان تصویر نگاشت گری از این کدها به‌دست آمده است.

فهرست منابع

[1] T. Blackford, *Negacyclic duadic codes*, Finite Fields and Their Applications, **14** (2008) 930-943.

[2] T. Blackford, *Isodual constacyclic codes*, Finite Fields and Their Applications, **24** (2013) 29-44.

[3] S. T. Dougherty, *Algebraic Coding Theory Over Finite Commutative Rings*, Springer, 2010.

[4] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole, *The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory, **40(2)** (1994) 301-319.

[5] W. C. Hufman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambrigde University press, 2003.

[6] A. Kaya, B. Yildiz, I. Siap, *Quadratic residue codes over $\mathbb{F}_p + u\mathbb{F}_p$ and their gray images*, Journal of Pure and Applied Algebra, **218** (2014) 1999-2011.

[7] J. S. Leon, J. M. Masley, V. Pless, *Duadic Codes*, IEEE Transactions on Information Theory, IT-30. (1984) 709–714.

[8] V. Pless, W. C. Hufman, *Handbook of Coding Theory*, Elsevier Science, Part 2, 1998.

[9] K. Samei, A. Soufi, *Quadratic residue codes over $\mathbb{F}_{p^r} + u_1\mathbb{F}_{p^r} + u_2\mathbb{F}_{p^r} + \cdots + u_t\mathbb{F}_{p^r}$*, Advances in Mathematics of Communications, **11(4)** (2017) 791-804.

[10] S. Zhu, L. Wang, *A class of constacyclic codes over $F_p + vF_p$ and its Gray image*, Discrete Mathematics, **311** (2011) 2677–2682.

A class of negacyclic duadic codes over ring $\mathbb{F}_q + v\mathbb{F}_q$ and their extensions

M. Golparian[1], R. Rezaei[1] † and K. Samei[2]

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

Communicated by: Mehrdad Namdari

Received: 2023/5/10 Accepted: 2023/6/6

Abstract: Blackford (2008) [1] introduced the concept of negacyclic duadic codes over the field $\mathbb{F}_q$, and classified all self-dual negacyclic codes over $\mathbb{F}_q$. In this paper, we define negacyclic duadic codes over ring $\mathbb{F}_q + v\mathbb{F}_q$ and by using a Gray map on these codes, we get self-dual and self-orthogonal codes on the field $\mathbb{F}_q$. Also, we introduce some extensions of negacyclic duadic codes over ring $\mathbb{F}_q + v\mathbb{F}_q$ and present their properties. Finally, we present some examples of negacyclic duadic codes over this ring and self-dual and self-orthogonal codes on the field $\mathbb{F}_q$.

Keywords: Negacyclic code, Self-dual code, Self-orthogonal code.

† Corresponding author.
E-mail addresses: ras_razaei@yahoo.com; r.rezaei@malayeru.ac.ir,