مجله مدل‌سازی پیشرفته ریاضی
سال ، دوره ، شماره ، ص

شاپا چاپی: ۲۲۵۱-۸
DOI:

خطی بودن تصویر گری همگن کدهای خطی روی $\mathbb{Z}_9$

علیرضا مهری[(۱)]، حمیدرضا عیوضی[(۱)] و کریم سامعی[(۱)]×

(۱) گروه ریاضی، دانشکده علوم پایه، دانشگاه بوعلی سینا، همدان، ایران

دبیر مسئول:

تاریخ دریافت: تاریخ پذیرش:

چکیده: کدهای $\mathbb{Z}_9$-جمعی به طول n زیرگروه‌هایی از $\mathbb{Z}_9^n$ هستند. فرض کنید $\mathcal{C}$ یک کد خطی به طول n روی $\mathbb{Z}_9$ و Φ نگاشت گری همگن روی $\mathbb{Z}_9^n$ باشد. در این مقاله، نشان می‌دهیم تصویر گری همگن $\mathcal{C}$ خطی است، اگر و تنها اگر برای هر $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$، $\boldsymbol{u} \circledast \boldsymbol{v} \in \mathcal{C}$. وقتی‌که $\mathcal{C}$ دوری و n نسبت به ۳ اول باشد، با استفاده از چندجمله‌ای مولد، یک شرط لازم و کافی برای خطی بودن تصویر گری همگن آن داده شده است. به عنوان یک نتیجه، نشان داده شده است که تصویر گری همگن یک کد باقیمانده مربعی روی $\mathbb{Z}_9$ خطی نیست.

واژه‌های کلیدی: کد دوری، نگاشت گری همگن، کد خطی، تبدیل متسون- سالومون.

رده‌بندی ریاضی: 94B15, 11T71.

۱ مقدمه

فرض کنید $\mathbb{F}_3$ میدان متناهی از مرتبه ۳، $\mathbb{Z}_9$ حلقه اعداد صحیح به پیمانه ۹ و n عدد صحیح مثبتی باشد. $\mathbb{F}_3^n$ و $\mathbb{Z}_9^n$ را به ترتیب مجموعه همه n تایی‌ها روی $\mathbb{F}_3$ و $\mathbb{Z}_9$ در نظر بگیرید. هر زیرمجموعه ناتهی $\mathcal{C}$ از $\mathbb{F}_3^n$ یک کد سه‌سه‌ای به طول n نامیده می‌شود و این کد خطی است، هرگاه یک فضای برداری باشد. یک زیرمجموعه ناتهی $\mathcal{C}$ از $\mathbb{Z}_9^n$ یک کد خطی روی $\mathbb{Z}_9$ نامیده می‌شود، اگر یک زیرگروه از $\mathbb{Z}_9^n$ باشد. یک کد خطی دوری نامیده می‌شود، اگر یک شیفت دوری از هر یک از کدواژه‌های آن یک کدواژه باشد. در این مقاله از حروف $\mathcal{C}$ و C به ترتیب برای نشان دادن کدهای روی $\mathbb{Z}_9$ و کدهای سه‌سه‌ای استفاده می‌کنیم. بر خلاف کدهای خطی روی میدان‌های متناهی، کدهای خطی روی حلقه‌ها پایه‌ای ندارند، اما دارای یک ماتریس مولد می‌باشند. یک ماتریس $k \times n$، $\mathcal{G}$ روی $\mathbb{Z}_9$ یک ماتریس مولد $\mathcal{C}$ نامیده می‌شود، هرگاه سطرهای $\mathcal{G}$، $\mathcal{C}$ را تولید کنند و هیچ زیرمجموعه سره‌ای از سطرهای $\mathcal{G}$، $\mathcal{C}$ را تولید نکند. یک کد خطی به طول n روی $\mathbb{Z}_9$ هم‌ارز جایگشتی با کدی با ماتریس مولد زیر است:

$$\mathcal{G} = \begin{bmatrix} I_{k_0} & A & B \\ 0 & 3I_{k_1} & 3F \end{bmatrix}, \tag{۱.۱}$$

× نویسنده مسئول مقاله

رایانامه: samei@basu.ac.ir

که در آن درایه‌های A و F از میدان $\mathbb{F}_۳$، و درایه‌های B از حلقه $\mathbb{Z}_۹$ هستند ([؟ ؟]). جمع در $\mathbb{F}_۳$ و $\mathbb{Z}_۹$ به ترتیب با "$\oplus$" و "$+$" نمایش داده می‌شود. برای هر $u \in \mathbb{Z}_۹$، بسط سه‌سه‌ای $u = u_۰ + ۳u_۱$ به صورت $[u]_۳ = [u_۰, u_۱]_۳$ نشان داده می‌شود، که در آن $u_۰$ و $u_۱$ متعلق به $\mathbb{F}_۳$ هستند.

نگاشت‌های گری مختلفی از $\mathbb{Z}_{p^s}$ به $\mathbb{F}_p^{p^{s-۱}}$ وجود دارد، که در آن s عددی صحیح و مثبت و p عددی اول است، برای نمونه [؟ ؟ ؟] را ببینید. تعریف نگاشت گری همگن ϕ از $\mathbb{Z}_۹$ به $\mathbb{F}_۳^۳$ به صورت تعریف شده در [؟] است؛ یعنی به صورت:

$$\phi(۰) = ۰۰۰, \phi(۱) = ۰۱۲, \phi(۲) = ۰۲۱, \phi(۳) = ۱۱۱, \phi(۴) = ۱۲۰, \phi(۵) = ۱۰۲,$$
$$\phi(۶) = ۲۲۲, \phi(۷) = ۲۰۱, \phi(۸) = ۲۱۰.$$

البته دقت داشته باشید که ϕ از $\mathbb{Z}_۹$ به $\mathbb{F}_۳^۳$ را می‌توان برای هر $r \in \mathbb{Z}_۹$ به صورت $\phi(r) = [r]_۳\mathcal{A}$ نیز نوشت که در آن

$$\mathcal{A} = \begin{bmatrix} ۰ & ۱ & ۲ \\ ۱ & ۱ & ۱ \end{bmatrix}.$$

همچنین، نگاشت Φ برای هر $\boldsymbol{z} = (z_۱, \ldots, z_n)$ متعلق به $\mathbb{Z}_۹^n$ را می‌توان به صورت زیر توسیع داد:

$$\begin{aligned} \Phi : \mathbb{Z}_۹^n &\longrightarrow \mathbb{F}_۳^{۳n} \\ \boldsymbol{z} &\longmapsto (\phi(z_۱), \ldots, \phi(z_n)). \end{aligned}$$

در حالت کلی، لازم نیست $\Phi(\mathcal{C})$ خطی باشد. یکی از موضوعات جالب در نظریه کدگذاری جبری بررسی شرایطی است که در آن بتوان خطی بودن یا نبودن تصویر یک کد خطی را مشخص کرد. برای کد خطی $\mathcal{C}$ روی $\mathbb{Z}_{۲^s}$، یک شرط لازم و کافی برای خطی بودن $\Phi(\mathcal{C})$ در [؟] بیان شده است. به ویژه، در [؟ ؟] برخی شرایط لازم و کافی برای خطی بودن تصویر گری همگن یک کد خطی چهارگانی داده شده است. در [؟ ؟ ؟] مسئله خطی بودن برای خانواده کدهای خطی هادامارد روی $\mathbb{Z}_{p^s}$، $\mathbb{Z}_{۲^s}$ و $\mathbb{Z}_۸$ مورد بررسی و مطالعه قرار گرفته است. به‌علاوه، با استفاده از سطرهای ماتریس مولد (به شکل استاندارد) کد $\mathcal{C}$ روی $\mathbb{Z}_۸$، یک شرط لازم و کافی برای خطی بودن $\Phi(\mathcal{C})$ در [؟] بیان شده است. به تازگی، یک شرط لازم و کافی برای خطی بودن تصویر گری همگن یک کد خطی روی حلقه گالوای $GR(۴, m)$ در [؟] داده شده است. خطی بودن تصویر گری یک کد دوری به طول فرد روی $\mathbb{Z}_۴$، $\mathbb{Z}_۸$ و $GR(۴, m)$ در [؟ ؟ ؟] مطالعه شده است.

این مقاله شامل بخش‌های زیر است. در بخش ۲، خطی بودن تصویر گری همگن یک کد خطی به طول n روی $\mathbb{Z}_۹$ بررسی شده است. در بخش ۳، شرطی را روی چندجمله‌ای مولد یک کد دوری به طول n، که n نسبت به ۳ اول است، روی $\mathbb{Z}_۹$ ارائه می‌کنیم که تصویر گری آن خطی شود. سرانجام، در بخش ۴، نتایج و تحقیقات بیشتری در این مبحث ارائه می‌دهیم.

۲ تصویر گری همگن کدهای خطی روی $\mathbb{Z}_۹$

در حالت کلی، اگر $\mathcal{C}$ یک کد خطی به طول n روی $\mathbb{Z}_۹$ باشد، $\Phi(\mathcal{C})$ لزوماً خطی نیست. در این بخش، روشی را ارائه خواهیم داد که می‌توان از آن برای بررسی خطی بودن و یا غیرخطی بودن $\Phi(\mathcal{C})$ استفاده کرد. دو تعریف زیر می‌تواند برای اثبات نتیجه اصلی این بخش مفید واقع گردد:

تعریف ۱.۲. برای هر x و y متعلق به $\mathbb{Z}_۹$، تعریف می‌کنیم:

$$x \circledast y = ۶(x^۲y + xy^۲ + xy).$$

با در نظر گرفتن $x *' y = ۲(x^۲y + xy^۲ + xy)$، داریم: $x \circledast y = ۳(x *' y)$. فرض کنید $[x_۰, x_۱]_۳$ و $[y_۰, y_۱]_۳$ بسط سه‌سه‌ای x و y باشند. بنابراین بسط سه‌سه‌ای $x \circledast y$ برابر $[۰, ۲(x_۰^۲y_۰ \oplus x_۰y_۰^۲ \oplus x_۰y_۰)]_۳$ است. می‌توان نشان داد $[x \circledast y]_۳ \oplus [y]_۳ \oplus [x]_۳ = [x + y]_۳$. به‌علاوه، می‌توان عملگر "$\circledast$" روی $\mathbb{Z}_۹$ را به

صورت طبیعی به $\mathbb{Z}_۹^n$ توسیع داد؛ یعنی، اگر $\boldsymbol{x} = (x^۱, \ldots, x^n)$ و $\boldsymbol{y} = (y^۱, \ldots, y^n)$ متعلق به $\mathbb{Z}_۹^n$ باشند، آنگاه $\boldsymbol{x} \circledast \boldsymbol{y} = (x^۱ \circledast y^۱, \ldots, x^n \circledast y^n)$. توجه کنید که $[\boldsymbol{x} + \boldsymbol{y}]_۳ = [\boldsymbol{x}]_۳ \oplus [\boldsymbol{y}]_۳ \oplus [\boldsymbol{x} \circledast \boldsymbol{y}]_۳$. همچنین، اگر U و V دو زیرمجموعه از $\mathbb{Z}_۹^n$ باشند، تعریف می‌کنیم:

$$U \circledast V = \{\boldsymbol{x} \circledast \boldsymbol{y} : \boldsymbol{x} \in U, \boldsymbol{y} \in V\}$$

و

$$U *' V = \{\boldsymbol{x} *' \boldsymbol{y} : \boldsymbol{x} \in U, \boldsymbol{y} \in V\}.$$

تذکر **۲.۲**. در [؟] برای هر $u = u_۰ + ۳u_۱$ و $v = v_۰ + ۳v_۱$ متعلق به $\mathbb{Z}_۹$، عملگر "$\odot_۳$" به صورت زیر تعریف شده است:

$$u \odot_۳ v = [t_۰, t_۱]$$

که در آن

$$t_i = \begin{cases} ۱ & u_i \oplus v_i \geq ۳, \\ ۰ & u_i \oplus v_i < ۳. \end{cases}$$

با استفاده از جداول زیر می‌توان مشاهده کرد که $u \circledast v = ۳(u \odot_۳ v)$.

u, v	$۳(u \odot_۳ v)$	$u \circledast v$
۱, ۱	۰	۰
۱, ۲	۳	۳
۱, ۳	۰	۰
۱, ۴	۰	۰
۱, ۵	۳	۳
۱, ۶	۰	۰
۱, ۷	۰	۰
۱, ۸	۳	۳
۲, ۲	۳	۳
۲, ۳	۰	۰
۲, ۴	۳	۳
۲, ۵	۳	۳

u, v	$۳(u \odot_۳ v)$	$u \circledast v$
۲, ۶	۰	۰
۲, ۷	۳	۳
۲, ۸	۳	۳
۳, ۳	۰	۰
۳, ۴	۰	۰
۳, ۵	۰	۰
۳, ۶	۰	۰
۳, ۷	۰	۰
۳, ۸	۰	۰
۴, ۴	۰	۰
۴, ۵	۳	۳
۴, ۶	۰	۰

u, v	$۳(u \odot_۳ v)$	$u \circledast v$
۴, ۷	۰	۰
۴, ۸	۳	۳
۵, ۵	۳	۳
۵, ۶	۰	۰
۵, ۷	۳	۳
۵, ۸	۳	۳
۶, ۶	۰	۰
۶, ۷	۰	۰
۶, ۸	۰	۰
۷, ۷	۰	۰
۷, ۸	۳	۳
۸, ۸	۳	۳

قضیه **۳.۲**. فرض کنید $\mathcal{C}$ یک کد خطی به طول n روی $\mathbb{Z}_۹$ باشد. در این صورت $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر برای هر $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$، $\boldsymbol{x} \circledast \boldsymbol{y} \in \mathcal{C}$.

اثبات. ابتدا برای هر $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_۹^n$، ثابت می‌کنیم:

$$\Phi(\boldsymbol{x} + \boldsymbol{y} - (\boldsymbol{x} \circledast \boldsymbol{y})) = \Phi(\boldsymbol{x}) \oplus \Phi(\boldsymbol{y}). \tag{۱.۲}$$

کافی است (؟؟) را برای حالت $n = ۱$ بررسی کنیم، در این صورت می‌توان آن را برای $\mathbb{Z}_۹^n$ به طور طبیعی اثبات نمود. واضح است که برای هر $w \in \mathbb{Z}_۹$ با بسط $[w]_۳ = [w_۰, w_۱]_۳$،

$$[-w]_۳ = [۲w_۰, ۲w_۰^۲ \oplus ۲w_۱]_۳.$$

از سوی دیگر، برای $x, y \in \mathbb{Z}_۹$ با بسطهای $[x_۰, x_۱]_۳$ و $[y_۰, y_۱]_۳$ داریم:

$$[x + y]_۳ = [x]_۳ \oplus [y]_۳ \oplus [x \circledast y]_۳ = [x_۰ \oplus y_۰, x_۱ \oplus y_۱ \oplus ۲(x_۰^۲ y_۰ \oplus x_۰ y_۰^۲ \oplus x_۰ y_۰)]_۳.$$

بنابراین:

$$
\begin{aligned}
&[x+y-(x\circledast y)]_{۳}=\\
&[x+y]_{۳}\oplus[-(x\circledast y)]_{۳}\oplus[(x+y)\circledast -(x\circledast y)]_{۳}=\\
&[x_{۰}\oplus y_{۰},x_{۱}\oplus y_{۱}\oplus ۲(x_{۰}^{۲}y_{۰}\oplus x_{۰}y_{۰}^{۲}\oplus x_{۰}y_{۰})]_{۳}\oplus[۰,x_{۰}^{۲}y_{۰}\oplus x_{۰}y_{۰}^{۲}\oplus x_{۰}y_{۰}]_{۳}\oplus[۰,۰]_{۳}=\\
&[x_{۰}\oplus y_{۰},x_{۱}\oplus y_{۱}]_{۳}=\\
&[x]_{۳}\oplus[y]_{۳}.
\end{aligned}
$$

با ضرب نمودن دو طرف رابطه بالا در ماتریس $\mathcal{A}$، داریم:

$$[x+y-(x\circledast y)]_{۳}\mathcal{A}=[x]_{۳}\mathcal{A}\oplus[y]_{۳}\mathcal{A}.$$

درنتیجه، $\Phi(x+y-(x\circledast y))=\Phi(x)\oplus\Phi(y)$. با توجه به (؟؟)، برای هر $\boldsymbol{x},\boldsymbol{y}\in\mathcal{C}$،

$$\Phi(\boldsymbol{x}+\boldsymbol{y}-(\boldsymbol{x}\circledast\boldsymbol{y}))=\Phi(\boldsymbol{x})\oplus\Phi(\boldsymbol{y}).$$

لذا برای هر $\boldsymbol{x},\boldsymbol{y}\in\mathcal{C}$، $\Phi(\boldsymbol{x}+\boldsymbol{y}-(\boldsymbol{x}\circledast\boldsymbol{y}))\in\Phi(\mathcal{C})$ اگر و تنها اگر $\Phi(\boldsymbol{x})\oplus\Phi(\boldsymbol{y})\in\Phi(\mathcal{C})$. اکنون اثبات کامل است. □

تعریف ۴.۲. فرض کنید $[u_{۰},u_{۱}]_{۳}$ و $[v_{۰},v_{۱}]_{۳}$ به ترتیب بسط‌های سه‌سه‌ای u و v به عنوان اعضای $\mathbb{Z}_{۹}$ باشند. عملگر "$\odot$" بین u و v را به صورت زیر تعریف می‌کنیم:

$$u\odot v=u_{۰}v_{۰}+۳u_{۱}v_{۱}.$$

در ادامه با استفاده از ماتریس مولد $\mathcal{C}$، یک شرط لازم و کافی ارائه می‌دهیم که می‌توان از آن برای بررسی خطی بودن و یا غیرخطی بودن $\Phi(\mathcal{C})$ بهره برد. بدین منظور، ابتدا لم زیر را بیان می‌کنیم:

لم ۵.۲. برای $\boldsymbol{x}_{۱},\boldsymbol{x}_{۲},\ldots,\boldsymbol{x}_{m},\boldsymbol{w}\in\mathbb{Z}_{۹}^{n}$، داریم:

$$(\sum_{i=۱}^{m}\boldsymbol{x}_{i})\circledast\boldsymbol{w}=\sum_{i=۱}^{m}(\boldsymbol{x}_{i}\circledast\boldsymbol{w})\oplus\sum_{۱\le j<l\le m}۳(\boldsymbol{x}_{j}\odot\boldsymbol{x}_{l}\odot\boldsymbol{w}).\qquad(۲.۲)$$

اثبات. کافی است (؟؟) را برای حالت $n=۱$ ثابت کنیم، می‌توان آن را برای $\mathbb{Z}_{۹}^{n}$ به صورت طبیعی اثبات نمود. فرض کنید $[u_{۰},u_{۱}]_{۳}$، $[v_{۰},v_{۱}]_{۳}$ و $[w_{۰},w_{۱}]_{۳}$ به ترتیب بسط سه‌سه‌ای u، v و w باشند. (؟؟) را با استقرا روی m ثابت می‌کنیم. برای $m=۲$، با به کار بردن رابطه

$$[u+v]_{۳}=[u]_{۳}\oplus[v]_{۳}\oplus[u\circledast v]_{۳}=[u_{۰}\oplus v_{۰},u_{۱}\oplus v_{۱}\oplus ۲(u_{۰}^{۲}v_{۰}\oplus u_{۰}v_{۰}^{۲}\oplus u_{۰}v_{۰})]_{۳}$$

و با استفاده از عملگر "$\circledast$"، خواهیم داشت:

$$
\begin{aligned}
&[(u+v)\circledast w]_{۳}=\\
&[۰,۲(u_{۰}\oplus v_{۰})^{۲}w_{۰}\oplus ۲(u_{۰}\oplus v_{۰})w_{۰}^{۲}\oplus ۲(u_{۰}\oplus v_{۰})w_{۰}]_{۳}=\\
&[۰,۲u_{۰}^{۲}w_{۰}\oplus ۴u_{۰}v_{۰}w_{۰}\oplus ۲v_{۰}^{۲}w_{۰}\oplus ۲u_{۰}w_{۰}^{۲}\oplus ۲v_{۰}w_{۰}^{۲}\oplus ۲u_{۰}w_{۰}\oplus ۲v_{۰}w_{۰}]_{۳}=\\
&[۰,۲u_{۰}^{۲}w_{۰}\oplus ۲u_{۰}w_{۰}^{۲}\oplus ۲u_{۰}w_{۰}]_{۳}\oplus[۰,۲v_{۰}^{۲}w_{۰}\oplus ۲v_{۰}w_{۰}^{۲}\oplus ۲v_{۰}w_{۰}]_{۳}\oplus[۰,u_{۰}v_{۰}w_{۰}]_{۳}=\\
&[u\circledast w]_{۳}\oplus[v\circledast w]_{۳}\oplus[۳(u\odot v\odot w)]_{۳}.
\end{aligned}
$$

فرض کنید فرض استقرا برای $m=k-۱$ برقرار باشد. برای $m=k$، نتیجه می‌گیریم که:

$$
\begin{aligned}
&(x_{۱}+x_{۲}+\cdots+x_{k-۱}+x_{k})\circledast w=\\
&((x_{۱}+x_{۲}+\cdots+x_{k-۱})\circledast w)\oplus(x_{k}\circledast w)\oplus ۳((x_{۱}+\cdots+x_{k-۱})\odot x_{k}\odot w).
\end{aligned}
$$

اکنون با استفاده از استقرا ثابت می‌کنیم:

$$۳((x_۱ + \cdots + x_{k-۱}) \odot x_k \odot w) = \sum_{i=۱}^{k-۱} ۳(x_i \odot x_k \odot w).$$

قرار می‌دهیم $k = ۳$، و $[x_{۱۰}, x_{۱۱}]_۳$، $[x_{۲۰}, x_{۲۱}]_۳$ و $[x_{۳۰}, x_{۳۱}]_۳$ را به ترتیب بسط سه‌سه‌ای $x_۱$، $x_۲$ و $x_۳$ در نظر می‌گیریم. با استفاده از عملگر "$\odot$" داریم:

$$\begin{aligned}[۳((x_۱ + x_۲) \odot x_۳ \odot w)]_۳ &= [۰, (x_{۱۰} \oplus x_{۲۰})x_{۳۰}w_۰]_۳ \\ &= [۰, x_{۱۰}x_{۳۰}w_۰]_۳ \oplus [۰, x_{۲۰}x_{۳۰}w_۰]_۳ \\ &= [۳(x_۱ \odot x_۳ \odot w)]_۳ \oplus [۳(x_۲ \odot x_۳ \odot w)]_۳.\end{aligned}$$

حال فرض کنید فرض استقرا برای $k - ۲$ برقرار باشد. برای $k - ۱$، داریم:

$$۳((x_۱ + \cdots + x_{k-۲} + x_{k-۱}) \odot x_k \odot w) = ۳((x_۱ + \cdots + x_{k-۲}) \odot x_k \odot w) \oplus ۳(x_{k-۱} \odot x_k \odot w).$$

با توجه به فرض استقرا (یعنی $k - ۲$)، نتیجه می‌گیریم:

$$\begin{aligned}&۳((x_۱ + \cdots + x_{k-۲} + x_{k-۱}) \odot x_k \odot w) = \\ &۳((x_۱ + \cdots + x_{k-۲}) \odot x_k \odot w) \oplus ۳(x_{k-۱} \odot x_k \odot w) = \\ &۳(x_۱ \odot x_k \odot w) \oplus ۳(x_۲ \odot x_k \odot w) \oplus \cdots \oplus ۳(x_{k-۲} \odot x_k \odot w) \oplus ۳(x_{k-۱} \odot x_k \odot w) = \\ &\sum_{i=۱}^{k-۱} ۳(x_i \odot x_k \odot w).\end{aligned}$$

از سوی دیگر، با استفاده از فرض استقرا (یعنی $m = k - ۱$)، داریم:

$$(x_۱ + \cdots + x_{k-۱}) \circledast w = \sum_{i=۱}^{k-۱} (x_i \circledast w) \oplus \sum_{۱ \le j < l \le k-۱} ۳(x_j \odot x_l \odot w).$$

درنتیجه:

$$(\sum_{i=۱}^{m} x_i) \circledast w = \sum_{i=۱}^{m} (x_i \circledast w) \oplus \sum_{۱ \le j < l \le m} ۳(x_j \odot x_l \odot w).$$

□

نتیجه ۶.۲. فرض کنید $\mathcal{C}$ یک کد خطی به طول n روی $\mathbb{Z}_۹$ با ماتریس مولد (۱.۱) باشد که در آن $\boldsymbol{v}_j$ و $\boldsymbol{u}_i$ بردارهایی در $\mathbb{Z}_۹^n$ به ترتیب از مرتبه ۹ و ۳ هستند. در این صورت $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر برای هر $۱ \le t \le l \le k_۰$، $\boldsymbol{v}_t \circledast \boldsymbol{v}_l \in \mathcal{C}$ و برای هر $۱ \le \alpha < \beta \le \gamma \le k_۰$، $۳(\boldsymbol{v}_\alpha \odot \boldsymbol{v}_\beta \odot \boldsymbol{v}_\gamma) \in \mathcal{C}$.

اثبات. فرض کنید $\mathcal{C}$ یک کد خطی به طول n روی $\mathbb{Z}_۹$ با ماتریس مولد (۱.۱) باشد، در این صورت هر کدواژه به صورت منحصربه‌فردی به شکل $\sum_{j=۱}^{k_۰} \mu_j \boldsymbol{v}_j + \sum_{i=۱}^{k_۱} \lambda_i \boldsymbol{u}_i$ قابل نمایش است، به‌طوری‌که برای $۱ \le j \le k_۰$، $\mu_j \in \mathbb{Z}_۹$، و برای $۱ \le i \le k_۱$، $\lambda_i \in \mathbb{F}_۳$. توجه کنید که اگر یکی از بردارهای $\boldsymbol{u}$، $\boldsymbol{v}$ یا $\boldsymbol{w}$ از مرتبه ۳ باشند، آنگاه $۳(\boldsymbol{u} \odot \boldsymbol{v} \odot \boldsymbol{w}) = \boldsymbol{u} \circledast \boldsymbol{v} = ۰$. لذا بنا بر قضیه ؟؟ و لم ؟؟، $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر برای هر t و l که در شرط $۱ \le t \le l \le k_۰$ صدق می‌کند، $\boldsymbol{v}_t \circledast \boldsymbol{v}_l \in \mathcal{C}$، و همچنین برای هر α، β و γ که در شرط $۱ \le \alpha < \beta \le \gamma \le k_۰$ صدق می‌کند، $۳(\boldsymbol{v}_\alpha \odot \boldsymbol{v}_\beta \odot \boldsymbol{v}_\gamma) \in \mathcal{C}$. □

مثال ۷.۲. فرض کنید $\mathcal{C}$ یک کد خطی به طول ۷ روی $\mathbb{Z}_۹$ با ماتریس مولد

$$\mathcal{G} = \begin{bmatrix} \boldsymbol{v}_۱ \\ \boldsymbol{v}_۲ \\ \boldsymbol{v}_۳ \\ \boldsymbol{u}_۱ \\ \boldsymbol{u}_۲ \end{bmatrix} = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۰ & ۴ & ۷ \\ ۰ & ۱ & ۰ & ۰ & ۲ & ۱ & ۸ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۵ & ۱ \\ ۰ & ۰ & ۰ & ۳ & ۰ & ۶ & ۳ \\ ۰ & ۰ & ۰ & ۰ & ۳ & ۳ & ۶ \end{bmatrix}$$

باشد. از آنجا که $\boldsymbol{v}_۱ \circledast \boldsymbol{v}_۲ = ۰۰۰۰۰۰۳ \notin \mathcal{C}$، لذا $\Phi(\mathcal{C})$ خطی نیست.

مثال **۸.۲**. فرض کنید $\mathcal{C}$ یک کد خطی به طول ۱۰ روی $\mathbb{Z}_۹$ با ماتریس مولد زیر باشد:

$$\mathcal{G} = \begin{bmatrix} \boldsymbol{v}_۱ \\ \boldsymbol{v}_۲ \\ \boldsymbol{v}_۳ \\ \boldsymbol{v}_۴ \end{bmatrix} = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۳ & ۶ & ۶ & ۳ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۶ & ۳ & ۶ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۳ & ۶ & ۳ & ۶ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۳ & ۳ & ۳ & ۶ \end{bmatrix}.$$

به سادگی می‌توان نشان داد که $\boldsymbol{v}_۱ \circledast \boldsymbol{v}_۱$، $\boldsymbol{v}_۲ \circledast \boldsymbol{v}_۲$، $\boldsymbol{v}_۳ \circledast \boldsymbol{v}_۳$، $\boldsymbol{v}_۴ \circledast \boldsymbol{v}_۴$، $\boldsymbol{v}_۱ \circledast \boldsymbol{v}_۲$، $\boldsymbol{v}_۱ \circledast \boldsymbol{v}_۳$، $\boldsymbol{v}_۱ \circledast \boldsymbol{v}_۴$، $\boldsymbol{v}_۲ \circledast \boldsymbol{v}_۳$، $\boldsymbol{v}_۲ \circledast \boldsymbol{v}_۴$، $\boldsymbol{v}_۳ \circledast \boldsymbol{v}_۴$، $۳(\boldsymbol{v}_۱ \odot \boldsymbol{v}_۱ \odot \boldsymbol{v}_۲)$، $۳(\boldsymbol{v}_۱ \odot \boldsymbol{v}_۱ \odot \boldsymbol{v}_۳)$، $۳(\boldsymbol{v}_۱ \odot \boldsymbol{v}_۱ \odot \boldsymbol{v}_۴)$، $۳(\boldsymbol{v}_۲ \odot \boldsymbol{v}_۲ \odot \boldsymbol{v}_۱)$، $۳(\boldsymbol{v}_۲ \odot \boldsymbol{v}_۲ \odot \boldsymbol{v}_۳)$، $۳(\boldsymbol{v}_۲ \odot \boldsymbol{v}_۲ \odot \boldsymbol{v}_۴)$، $۳(\boldsymbol{v}_۳ \odot \boldsymbol{v}_۳ \odot \boldsymbol{v}_۱)$، $۳(\boldsymbol{v}_۳ \odot \boldsymbol{v}_۳ \odot \boldsymbol{v}_۲)$، $۳(\boldsymbol{v}_۳ \odot \boldsymbol{v}_۳ \odot \boldsymbol{v}_۴)$، $۳(\boldsymbol{v}_۴ \odot \boldsymbol{v}_۴ \odot \boldsymbol{v}_۱)$، $۳(\boldsymbol{v}_۴ \odot \boldsymbol{v}_۴ \odot \boldsymbol{v}_۲)$، $۳(\boldsymbol{v}_۴ \odot \boldsymbol{v}_۴ \odot \boldsymbol{v}_۳)$، $۳(\boldsymbol{v}_۱ \odot \boldsymbol{v}_۲ \odot \boldsymbol{v}_۳)$، $۳(\boldsymbol{v}_۱ \odot \boldsymbol{v}_۲ \odot \boldsymbol{v}_۴)$، $۳(\boldsymbol{v}_۱ \odot \boldsymbol{v}_۳ \odot \boldsymbol{v}_۴)$ و $۳(\boldsymbol{v}_۲ \odot \boldsymbol{v}_۳ \odot \boldsymbol{v}_۴)$ متعلق به $\mathcal{C}$ هستند؛ لذا $\Phi(\mathcal{C})$ خطی است.

۳ تصویر گری همگن کدهای دوری روی $\mathbb{Z}_۹$

همه کدهای دوری به طول فرد روی $\mathbb{Z}_۴$ که تصویر گری آنها خطی است، توسط ولفمن شناسایی شده است ([؟]). در سرتاسر این بخش فرض می‌کنیم $\gcd(n, ۳) = ۱$. حلقه‌های خارج قسمتی $\frac{\mathbb{Z}_۹[x]}{\langle x^n - ۱\rangle}$ و $\frac{\mathbb{F}_۳[x]}{\langle x^n - ۱\rangle}$ به ترتیب با $R_{۲,n}$ و $R_{۱,n}$ نشان داده می‌شوند. همریختی طبیعی $\mathbb{Z}_۹ \longrightarrow \mathbb{F}_۳$: $^-$با ضابطه $c_۰ + ۳c_۱ \longmapsto c_۰$، را می‌توان به یک برووریختی حلقه‌ای از $\mathbb{Z}_۹[x]$ به $\mathbb{F}_۳[x]$ با ضابطه زیر گسترش داد:

$$\begin{aligned} ^-\colon \mathbb{Z}_۹[x] &\longrightarrow \mathbb{F}_۳[x] \\ a_۰ + a_۱x + \cdots + a_nx^n &\longmapsto \bar{a}_۰ + \bar{a}_۱x + \cdots + \bar{a}_nx^n. \end{aligned} \tag{۱.۳}$$

به سادگی می‌توان دید که برای هر $r(x) \in \mathbb{Z}_۹[x]$، $۳r(x) = ۳\bar{r}(x)$. اگر $\bar{u}(x)$ و $\bar{v}(x)$ متعلق به $R_{۱,n}$ باشند، آنگاه $۳\bar{u}(x) = ۳\bar{v}(x)$ در $R_{۲,n}$ نتیجه می‌دهد که $\bar{u}(x) = \bar{v}(x)$. برای هر $\bar{r}(x) \in R_{۱,n}$، $\langle \bar{r}(x)\rangle_۳$ ایده‌آل اصلی تولید شده توسط $\bar{r}(x)$ است. فرض کنید R، حلقه $\mathbb{Z}_۹$ یا میدان $\mathbb{F}_۳$ باشد. نمایش چندجمله‌ای R^n، با نگاشت $\mathcal{P}$ از R^n به $R_{۱,n}$ یا $R_{۲,n}$ با ضابطه $\mathcal{P}(a_۰, a_۱, \ldots, a_{n-۱}) = \sum_{i=۰}^{n-۱} a_ix^i$ نشان داده می‌شود. توجه کنید که $\mathcal{P}_۳^n$ و $\mathcal{P}_۹^n$ به ترتیب نمایش چندجمله‌ای‌های $\mathbb{F}_۳^n$ و $\mathbb{Z}_۹^n$ هستند. چندجمله‌ای‌های $f_۱(x)$ و $f_۲(x)$ نسبت به هم اول در $\mathbb{Z}_۹[x]$ نامیده می‌شوند، اگر چندجمله‌ای‌های $\lambda_۱(x)$ و $\lambda_۲(x)$ در $\mathbb{Z}_۹[x]$ وجود داشته باشند؛ به‌طوری‌که $\lambda_۱(x)f_۱(x) + \lambda_۲(x)f_۲(x) = ۱$، یا به طور معادل $\mathbb{Z}_۹[x]f_۱(x) + \mathbb{Z}_۹[x]f_۲(x) = \mathbb{Z}_۹[x]$. در این بخش، ایده ولفمن را برای کدهای به طول n روی $\mathbb{Z}_۹$ تعمیم می‌دهیم. یادآوری می‌کنیم که یک کد خطی $\mathcal{C}$ به طول n دوری نامیده می‌شود، اگر $(c_۰, \ldots, c_{n-۱}) \in \mathcal{C}$ نتیجه دهد $(c_{n-۱}, \ldots, c_{n-۲}) \in \mathcal{C}$. توجه کنید که $R_{۲,n}$ یک حلقه ایده‌آل اصلی است ([؟]).

در ابتدا، ساختار کد دوری در حلقه $\mathbb{Z}_۹$ را در گزاره زیر بیان می‌کنیم:

گزاره **۱.۳**. ([؟]) فرض کنید $\mathcal{C}$ یک کد دوری به طول n روی $\mathbb{Z}_۹$ باشد. در این صورت، مجموعه‌ای از چندجمله‌ای‌های دو به دو نسبت به هم اول $f_۰(x)$، $f_۱(x)$ و $f_۲(x)$ (احتمالا برابر با ۱) وجود دارد به‌طوری‌که $f_۰(x)f_۲(x)f_۱(x) = x^n - ۱$، و $\mathcal{C}$ توسط $\{\hat{f}_۲(x), ۳\hat{f}_۱(x)\}$ تولید می‌شود، به‌طوری‌که برای $۱ \le i \le ۲$، $\hat{f}_i(x)$ عبارت است از حاصلضرب همه $f_j(x)$ ها، بجز $f_i(x)$؛ یعنی، $\mathcal{C} = \langle f_۰(x)f_۱(x), ۳f_۰(x)f_۲(x)\rangle$.

گزاره **۲.۳**. ([؟]) یک زیرمجموعه از $\mathbb{Z}_۹^n$ یک کد دوری خطی به طول n روی $\mathbb{Z}_۹$ است، اگر و تنها اگر نمایش چندجمله‌ای آن یک ایده‌آل از $R_{۲,n}$ باشد.

همانند قضیه ۴ و لم ۶ در [؟] داریم:

لم **۳.۳**. با فرض برقرار بودن شرایط گزاره ؟؟، می‌توان نتیجه گرفت:

(i) $\mathcal{C} = \langle f_۰(x)f_۱(x), ۳f_۰(x)\rangle = \langle f_۰(x)f_۱(x) + ۳f_۰(x)\rangle$.

(ii) $\mathcal{C} \cap ۳R_{۲,n} = \langle ۳f_۰(x) \rangle$.

اثبات. (i) با استفاده از گزاره ؟؟، $\mathcal{C} = \langle f_۰(x)f_۱(x), ۳f_۰(x)f_۲(x) \rangle$ و $x^n - ۱ = f_۰(x)f_۲(x)f_۱(x)$. قرار دهید $\mathcal{C}' = \langle f_۰(x)f_۱(x), ۳f_۰(x) \rangle$، به وضوح $\mathcal{C} \subseteq \mathcal{C}'$. از آنجا که $gcd(f_۱(x), f_۲(x)) = ۱$، $r_۱(x)$ و $r_۲(x)$ متعلق به $\mathbb{Z}_۹[x]$ وجود دارند به‌طوری‌که:

$$r_۱(x)f_۱(x) + r_۲(x)f_۲(x) = ۱.$$

با ضرب دو طرف معادله بالا در $۳f_۰(x)$، داریم:

$$۳f_۰(x) = ۳r_۱(x)f_۰(x)f_۱(x) + ۳r_۲(x)f_۰(x)f_۲(x) \in \mathcal{C}.$$

بنابراین $\mathcal{C}' \subseteq \mathcal{C}$.
برای تساوی آخر، کافی است نشان دهیم که $\mathcal{C} \subseteq \langle g(x) \rangle$، که در آن $g(x) = f_۰(x)f_۱(x) + ۳f_۰(x)$.
از آنجا که $gcd(f_۱(x), ۳) = ۱$، $r_۱(x)$ و $r_۲(x)$ متعلق به $\mathbb{Z}_۹[x]$ وجود دارند به‌طوری‌که:

$$۳r_۲(x) + r_۱(x)f_۱(x) = ۱.$$

با ضرب دو طرف تساوی اخیر در $f_۰(x)f_۱(x)$، داریم:

$$f_۰(x)f_۱(x) = ۳f_۰(x)f_۱(x)r_۲(x) + f_۰(x)(f_۱(x))^۲ r_۱(x) \in \langle g(x) \rangle.$$

از سوی دیگر، $gcd(f_۰(x), f_۱(x)) = ۱$، بنابراین $s_۰(x), s_۱(x) \in \mathbb{Z}_۹[x]$ وجود دارند به‌طوری‌که:

$$s_۰(x)f_۰(x) + s_۱(x)f_۱(x) = ۱.$$

با ضرب دو طرف تساوی بالا در $۳f_۰(x)$، داریم:

$$۳f_۰(x) = ۳s_۰(x)(f_۰(x))^۲ + ۳s_۱(x)f_۰(x)f_۱(x) \in \langle g(x) \rangle$$

درنتیجه $\mathcal{C} = \langle g(x) \rangle$.

(ii) به سادگی می‌توان دید $\langle ۳f_۰(x) \rangle \subseteq \mathcal{C} \cap ۳R_{۲,n}$. فرض کنید $b(x) \in \mathcal{C} \cap ۳R_{۲,n}$، بنابراین، $r(x) \in R_{۲,n}$ وجود دارد به‌طوری‌که $b(x) = r(x)f_۰(x)f_۱(x) + ۳r(x)f_۰(x)$، لذا $r'(x) \in R_{۲,n}$ وجود دارد به گونه‌ای‌که $r(x) = ۳r'(x)$. درنتیجه، $b(x) = ۳r'(x)f_۰(x)f_۱(x) \in \langle ۳f_۰(x) \rangle$.

□

گزاره **۴.۳.** $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر $\langle \bar{f}_۰(x)\bar{f}_۱(x) \rangle_۳ *' \langle \bar{f}_۰(x)\bar{f}_۱(x) \rangle_۳ \subseteq \langle \bar{f}_۰(x)\bar{f}_۱(x) \rangle_۳$.

اثبات. با توجه به قضیه ؟؟ $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر برای هر $\boldsymbol{u}$ و $\boldsymbol{v}$ متعلق به $\mathcal{C}$، $\boldsymbol{u} \circledast \boldsymbol{v}$ متعلق به $\mathcal{C}$ باشد. از این رو، $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر برای هر $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$، $۳(\boldsymbol{u} *' \boldsymbol{v}) \in \mathcal{C}$. بنابراین، $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر برای هر $m_۱(x), m_۲(x) \in R_{۲,n}$، $۳(m_۱(x)g(x) *' m_۲(x)g(x)) \in \mathcal{C}$. از آنجا که $۳(m_۱(x)g(x) *' m_۲(x)g(x)) \in ۳R_{۲,n}$، برای هر $m_۱(x)$ و $m_۲(x)$ متعلق به $R_{۲,n}$، داریم:

$$۳(m_۱(x)g(x) *' m_۲(x)g(x)) \in \mathcal{C} \cap ۳R_{۲,n} = \langle ۳f_۰(x) \rangle.$$

پس $\Phi(\mathcal{C})$ خطی است؛ اگر و تنها اگر برای هر $m_۱(x), m_۲(x) \in R_{۲,n}$،

$$۳(m_۱(x)g(x) *' m_۲(x)g(x)) \in \langle ۳f_۰(x) \rangle,$$

اگر و تنها اگر برای هر $m_۱(x), m_۲(x) \in R_{۱,n}$،

$$\bar{m}_۱(x)\bar{g}(x) *' \bar{m}_۲(x)\bar{g}(x) \in \langle \bar{f}_۰(x) \rangle_۳,$$

اگر و تنها اگر برای هر $m_1(x), m_2(x) \in R_{1,n}$،

$$\bar{m}_1(x)\bar{f}_0(x)\bar{f}_1(x) *' \bar{m}_2(x)\bar{f}_0(x)\bar{f}_1(x) \in \langle \bar{f}_0(x)\rangle_3.$$

□

ملاحظه **۵.۳.** فرض کنید $\mathbb{F}_{3^t}$ میدان تجزیه‌گر $x^n - 1$ روی $\mathbb{F}_3$ و β یک ریشه n ام اولیه واحد در $\mathbb{F}_{3^t}$ باشد. تبدیل متسون– سالومون را به صورت تابع $\mathcal{T} : \frac{\mathbb{F}_{3^t}[x]}{\langle x^n-1\rangle} \longrightarrow \frac{\mathbb{F}_{3^t}[x]}{\langle x^n-1\rangle}$ تعریف می‌کنیم به گونه‌ای‌که:

$$U(x) = \mathcal{T}(u(x)) = \sum_{k=0}^{n-1} u(\beta^{-k})x^k.$$

به سادگی می‌توان بررسی کرد که $\mathcal{T}$ دوسویی است. تبدیل وارون $\mathcal{T}$ نیز به صورت زیر تعریف می‌شود:

$$u(x) = \mathcal{T}^{-1}(U(x)) = \sum_{k=0}^{n-1} U(\beta^k)x^k.$$

لم **۶.۳.** فرض کنید $U(x)$ و $V(x)$ متعلق به $\frac{\mathbb{F}_{3^t}[x]}{\langle x^n-1\rangle}$ باشند، آنگاه:

$$\mathcal{T}^{-1}(U(x) *' V(x)) = 2\mathcal{T}^{-1}(U(x))\mathcal{T}^{-1}(U(x)V(x) + (V(x))^2 + V(x)).$$

اثبات. در ابتدا برای $u(x), v(x) \in \frac{\mathbb{F}_{3^t}[x]}{\langle x^n-1\rangle}$، نشان می‌دهیم:

$$\mathcal{T}(u(x)) *' \mathcal{T}(v(x)) = 2\mathcal{T}(u(x)(u(x)v(x) + (v(x))^2 + v(x))).$$

$$\begin{aligned}
&\mathcal{T}(u(x)) *' \mathcal{T}(v(x)) = \\
&u(1) *' v(1) + (u(\beta^{-1}) *' v(\beta^{-1}))x + \cdots + (u(\beta^{-(n-1)}) *' v(\beta^{-(n-1)}))x^{n-1} = \\
&2((u(1))^2v(1) + u(1)(v(1))^2 + u(1)v(1)) \\
&+ (2((u(\beta^{-1}))^2v(\beta^{-1}) + u(\beta^{-1})(v(\beta^{-1}))^2 + u(\beta^{-1})v(\beta^{-1})))x \\
&+ \cdots + \\
&(2((u(\beta^{-(n-1)}))^2v(\beta^{-(n-1)}) + u(\beta^{-(n-1)})(v(\beta^{-(n-1)}))^2 + u(\beta^{-(n-1)})v(\beta^{-(n-1)})))x^{n-1} = \\
&2(u(1)(u(1)v(1) + v(1)v(1) + v(1)) \\
&+ (u(\beta^{-1})(u(\beta^{-1})v(\beta^{-1}) + v(\beta^{-1})v(\beta^{-1}) + v(\beta^{-1}))x \\
&+ \cdots + \\
&(u(\beta^{-(n-1)})(u(\beta^{-(n-1)})v(\beta^{-(n-1)}) + v(\beta^{-(n-1)})v(\beta^{-(n-1)}) + v(\beta^{-(n-1)})))x^{n-1}) = \\
&2\mathcal{T}(u(x)(u(x)v(x) + (v(x))^2 + v(x))).
\end{aligned}$$

درنتیجه داریم:

$$\mathcal{T}^{-1}(U(x) *' V(x)) = 2\mathcal{T}^{-1}(U(x))\mathcal{T}^{-1}(U(x)V(x) + (V(x))^2 + V(x)).$$

□

فرض کنید $\bar{u}(x)$ یک شمارنده $x^n - 1$ روی $\mathbb{F}_3$ و β یک ریشه n ام اولیه واحد روی $\mathbb{F}_3$ باشد. در این صورت، $(\bar{u} \otimes \bar{u})(x)$ شمارنده $x^n - 1$ روی $\mathbb{F}_3$ با ریشه‌های $\beta^i\beta^j$ است؛ به‌طوری‌که β^i و β^j ریشه‌های $\bar{u}(x)$ هستند.

لم ۷.۳. فرض کنید $\bar{d}(x)$ و $\bar{c}(x)$ چندجمله‌ای‌هایی در $\mathbb{F}_3[x]$ باشند به‌طوری‌که $x^n-1=\bar{d}(x)\bar{c}(x)$، و همچنین $\bar{e}(x)$ به گونه‌ای باشد که $x^n-1=(\bar{c}\otimes\bar{c})(x)\bar{e}(x)$. در این صورت، $\langle\bar{d}(x)\rangle_3 *' \langle\bar{d}(x)\rangle_3 \subseteq \langle\bar{e}(x)\rangle_3$.

اثبات. فرض کنید $\bar{s}(x)=\bar{m}_1(x)\bar{d}(x) *' \bar{m}_2(x)\bar{d}(x)$ متعلق به $\langle\bar{d}(x)\rangle_3 *' \langle\bar{d}(x)\rangle_3$ باشد، که در آن

$$m_1(x), m_2(x) \in R_{2,n}.$$

با استفاده از وارون تبدیل متسون- سالومون داریم:

$$\begin{aligned}\mathcal{T}^{-1}(\bar{s}(x)) &= \mathcal{T}^{-1}(\bar{m}_1(x)\bar{d}(x) *' \bar{m}_2(x)\bar{d}(x))\\ &= 2\mathcal{T}^{-1}(\bar{m}_1(x)\bar{d}(x))\mathcal{T}^{-1}(\bar{m}_1(x)\bar{d}(x)\bar{m}_2(x)\bar{d}(x)+\bar{m}_2^2(x)\bar{d}^2(x)+\bar{m}_2(x)\bar{d}(x)).\end{aligned}$$

درنتیجه:

$$\sum_{k=0}^{n-1}\bar{s}(\beta^k)x^k =$$
$$2((\sum_{i=0}^{n-1}\bar{m}_1(\beta^i)\bar{d}(\beta^i)x^i)(\sum_{j=0}^{n-1}(\bar{m}_1(\beta^j)\bar{m}_2(\beta^j)\bar{d}^2(\beta^j)+\bar{m}_2^2(\beta^j)\bar{d}^2(\beta^j)+\bar{m}_2(\beta^j)\bar{d}(\beta^j))x^j)).$$

توجه کنید که $\bar{d}(\beta^t)\neq 0$ اگر و تنها اگر $\bar{c}(\beta^t)=0$. بنابراین:

$$\sum_{k=0}^{n-1}\bar{s}(\beta^k)x^k = ((\sum_{\bar{c}(\beta^i)=0}\bar{m}_1(\beta^i)\bar{d}(\beta^i)x^i)(\sum_{\bar{c}(\beta^j)=0}(\bar{m}_1(\beta^j)\bar{m}_2(\beta^j)\bar{d}^2(\beta^j)+\bar{m}_2^2(\beta^j)\bar{d}^2(\beta^j)+\bar{m}_2$$
$$(\beta^j)\bar{d}(\beta^j))x^j)) = 2\sum_{(\bar{c}\otimes\bar{c})(\beta^k)=0}\sum_{i+j=k}((\bar{m}_1(\beta^i)\bar{d}(\beta^i))((\bar{m}_1(\beta^j)\bar{m}_2(\beta^j)\bar{d}^2(\beta^j)+\bar{m}_2^2(\beta^j)\bar{d}^2(\beta^j)+$$
$$\bar{m}_2(\beta^j)\bar{d}(\beta^j)))x^k.$$

با فرض $\bar{s}(\beta^k)\neq 0$، داریم $(\bar{c}\otimes\bar{c})(\beta^k)=0$؛ یا به طور معادل، اگر $\bar{e}(\beta^k)=0$، آنگاه $\bar{s}(\beta^k)=0$. لذا نتیجه می‌گیریم که $\bar{s}(x)\mid\bar{e}(x)$. بنابراین $\bar{s}(x)\in\langle\bar{e}(x)\rangle_3$. □

قضیه ۸.۳. چندجمله‌ای‌های $f_0(x)$، $f_1(x)$ و $f_2(x)$ را در نظر بگیرید به‌طوری‌که $x^n-1=f_0(x)f_2(x)f_1(x)$. فرض کنید $\mathcal{C}=\langle f_0(x)f_1(x)+3f_0(x)\rangle$ یک کد دوری خطی به طول n روی $\mathbb{Z}_9$ باشد، و $\bar{e}(x)$ به گونه‌ای باشد که $x^n-1=(\bar{f}_2\otimes\bar{f}_2)(x)\bar{e}(x)$. در این صورت، $\Phi(\mathcal{C})$ خطی است اگر و تنها اگر در $\mathbb{F}_3[x]$، $\bar{f}_0(x)\mid\bar{e}(x)$.

اثبات. اگر $\bar{f}_0(x)=1$ یا $\bar{f}_2(x)=1$، آنگاه $\bar{f}_0(x)\mid\bar{e}(x)$. لذا فرض کنید $\bar{f}_0(x)\neq 1$ و $\bar{f}_2(x)\neq 1$. قرار دهید:

$$K=\{k:(\bar{f}_2\otimes\bar{f}_2)(\beta^k)=0,\ 0\leq k\leq n-1\},$$
$$J(k)=\{j:\bar{f}_2(\beta^j)=\bar{f}_2(\beta^{k-j})=0,\ 0\leq j\leq n-1\}.$$

از آنجا که $\bar{f}_2(x)\neq 1$، نتیجه می‌گیریم $K\neq\emptyset$. اگر $k\in K$، داریم $J(k)\neq\emptyset$. با توجه به گزاره ؟؟، برای هر $0\leq j\leq n-1$، $\lambda_m(x)$ وجود دارد به‌طوری‌که $\bar{\lambda}_m(x)\bar{f}_0(x)=\bar{f}_0(x)\bar{f}_1(x) *' x^m\bar{f}_0(x)\bar{f}_1(x)$. با استفاده از وارون تبدیل متسون- سالومون و با فرض $\bar{d}(x)=\bar{f}_0(x)\bar{f}_1(x)$، داریم:

$$\sum_{k=0}^{n-1}\bar{\lambda}_m(\beta^k)\bar{f}_0(\beta^k)x^k =$$
$$\mathcal{T}^{-1}(\bar{f}_0(x)\bar{f}_1(x) *' x^m\bar{f}_0(x)\bar{f}_1(x)) =$$
$$2\mathcal{T}^{-1}(\bar{f}_0(x)\bar{f}_1(x))\mathcal{T}^{-1}((\bar{f}_0(x)\bar{f}_1(x))^2x^m+(x^m\bar{f}_0(x)\bar{f}_1(x))^2+x^m\bar{f}_0(x)\bar{f}_1(x)) =$$
$$2((\sum_{i=0}^{n-1}\bar{d}(\beta^i)x^i)(\sum_{j=0}^{n-1}(\bar{d}^2(\beta^j)(\beta^m)^j+\bar{d}^2(\beta^j)(\beta^m)^{2j}+\bar{d}(\beta^j)(\beta^m)^j)x^j)).$$

بنابراین:

$$\sum_{k\in K}\bar{\lambda}_m(\beta^k)\bar{f}_\circ(\beta^k)x^k = \\ ۲\sum_{k\in K}(\sum_{j\in J(k)}(\bar{d}(\beta^i)\bar{d}^۲(\beta^j)(\beta^m)^j + \bar{d}(\beta^i)\bar{d}^۲(\beta^j)(\beta^m)^{۲j} + \bar{d}(\beta^i)\bar{d}(\beta^j)(\beta^m)^j))x^k. \qquad (۲.۳)$$

فرض کنید $k\in K$ و $S_k(X)=\sum_{j\in J(K)}۲(\bar{d}(\beta^i)\bar{d}^۲(\beta^j)+\bar{d}(\beta^i)\bar{d}^۲(\beta^j)(\beta^m)^j+\bar{d}(\beta^i)\bar{d}(\beta^j))X^j$، لذا برای هر $k\in K$ و $j\in J(K)$، داریم $۲(\bar{d}(\beta^i)\bar{d}^۲(\beta^j)+\bar{d}(\beta^i)\bar{d}^۲(\beta^j)(\beta^m)^j+\bar{d}(\beta^i)\bar{d}(\beta^j))\neq ۰$، بنابراین، $S_k(X)\neq ۰$. از آنجا که درجه $S_k(X)$ حداکثر برابر با تعداد ریشه‌های $S_k(X)$ (یعنی، $n-۱$) است، لذا $۰\leq m\leq n-۱$ وجود دارد به‌طوری‌که $S_k(\beta^m)\neq ۰$. با استفاده از (؟؟) نتیجه می‌گیریم که $\bar{\lambda}_m(\beta^k)\bar{f}_\circ(\beta^k)\neq ۰$، این نتیجه می‌دهد که $\bar{f}_\circ(\beta^k)\neq ۰$. بنابراین $(\bar{f}_۲\otimes\bar{f}_۲)(\beta^k)=۰$ دلالت دارد بر اینکه $\bar{f}_\circ(\beta^k)\neq ۰$، یا به طور معادل $\bar{f}_\circ(\beta^k)=۰$ نتیجه می‌دهد که $(\bar{f}_۲\otimes\bar{f}_۲)(\beta^k)\neq ۰$. به بیان دیگر، اگر $\bar{f}_\circ(\beta^k)=۰$، آنگاه $\bar{e}(\beta^k)=۰$؛ یعنی $\bar{f}_\circ(x)\mid\bar{e}(x)$.

برعکس، اگر $\bar{f}_\circ(x)\mid\bar{e}(x)$، آنگاه $\langle\bar{e}(x)\rangle\subseteq\langle\bar{f}_\circ(x)\rangle$، با استفاده از لم ؟؟، $\langle\bar{d}(x)\rangle*'\langle\bar{d}(x)\rangle\subseteq\langle\bar{e}(x)\rangle$، لذا کافی است قرار دهیم $\bar{d}(x)=\bar{f}_\circ(x)\bar{f}_۱(x)$، بنابراین $\langle\bar{f}_\circ(x)\bar{f}_۱(x)\rangle*'\langle\bar{f}_\circ(x)\bar{f}_۱(x)\rangle\subseteq\langle\bar{e}(x)\rangle\subseteq\langle\bar{f}_\circ(x)\rangle$. با استفاده از گزاره ؟؟، نتیجه می‌گیریم که $\Phi(\mathcal{C})$ خطی است. □

نتیجه ۹.۳. فرض کنید $\mathcal{C}=\langle f_\circ(x)f_۱(x)+۳f_\circ(x)\rangle$ یک کد دوری به طول n روی $\mathbb{Z}_۹$ باشد، به‌طوری‌که $x^n-۱=f_\circ(x)f_۲(x)f_۱(x)$. در این صورت:

(i) اگر $f_\circ(x)=۱$، آنگاه $\Phi(\mathcal{C})$ خطی است.

(ii) اگر $f_۲(x)=۱$، آنگاه $\Phi(\mathcal{C})$ خطی است.

(iii) اگر $f_۲(x)=x-۱$، آنگاه $\Phi(\mathcal{C})$ خطی است.

مثال ۱۰.۳. در $\mathbb{Z}_۹[x]$، تجزیه $x^۴-۱$ به صورت زیر است:

$$(x-۸)(x^۲+۱)(x+۸)=f_\circ(x)f_۲(x)f_۱(x),$$

که در آن $f_\circ(x)=x-۸$، $f_۲(x)=x^۲+۱$ و $f_۱(x)=x+۸$. به سادگی می‌توان نشان داد که $f_۲(x)$، $f_\circ(x)$ و $f_۱(x)$ دو به دو نسبت به هم اول هستند. فرض کنید $\mathcal{C}$ یک کد دوری به طول ۴ روی $\mathbb{Z}_۹$ با چندجمله‌ای مولد $g(x)=f_\circ(x)f_۱(x)+۳f_\circ(x)$ باشد. به وضوح، $\bar{f}_\circ(x)$، $\bar{e}(x)=(x+۱)(x+۲)$ را در $\mathbb{F}_۳[x]$ می‌شمارد. بنا بر قضیه ؟؟، $\Phi(\mathcal{C})$ خطی است.

مثال ۱۱.۳. فرض کنید p یک عدد اول، و $\mathcal{Q}_p$ و $\mathcal{N}_p$ به ترتیب مجموعه‌های ناتهی باقیمانده مربعی و ناباقیمانده مربعی به پیمانه p باشند. فرض کنید $\mathcal{C}$ یک کد دوری به طول p روی $\mathbb{Z}_۹$ با چندجمله‌ای مولد

$$g(x)=f_\circ(x)f_۱(x)+۳f_\circ(x)$$

باشد، که در آن $f_۱(x)=۱$. قرار دهید $T=\{i+j:\bar{f}_۲(\beta^i)=\bar{f}_۲(\beta^j)=۰,\ ۰\leq i,j\leq n-۱\}$. از آنجا که $T=\{i+j:i,j\in\mathcal{N}_p\cup\{۰\}\}$، می‌توان نتیجه گرفت $|T|>\frac{p}{۲}$، لذا $T\cap\mathcal{Q}_p$ ناتهی است. این نتیجه می‌دهد که در $\mathbb{F}_۳[x]$، $\bar{f}_\circ(x)\nmid\bar{e}(x)$. لذا، $\Phi(\mathcal{C})$ خطی نیست. به سادگی می‌توان دید $\mathcal{C}=\langle f_\circ(x)\rangle$ یک کد باقیمانده مربعی به طول p روی $\mathbb{Z}_۹$ است ([؟]). درنتیجه، تصویر گری همگن یک کد باقیمانده مربعی روی $\mathbb{Z}_۹$ غیرخطی است.

۴ نتیجه

برای یک کد خطی $\mathcal{C}$ روی $\mathbb{Z}_۹$، نشان دادیم که تصویر گری همگن $\mathcal{C}$ خطی است اگر و تنها اگر برای هر $\boldsymbol{u},\boldsymbol{v}\in\mathcal{C}$، $\boldsymbol{u}\circledast\boldsymbol{v}\in\mathcal{C}$. همچنین، یک شرط لازم و کافی برای خطی بودن تصویر گری همگن یک کد دوری به طول n (نسبت به ۳ اول است) روی $\mathbb{Z}_۹$ با استفاده از چندجمله‌ای مولد آن کد ارائه کردیم. به منظور تحقیقات بیشتر، بررسی خطی بودن تصویر گری همگن یک کد خطی و یک کد دوری روی $\mathbb{Z}_{۳^s}$ $(s>۲)$، به ترتیب با استفاده از ماتریس مولد و چندجمله‌ای مولد این کدها جالب خواهند بود.

فهرست منابع

[1] D. K. Bhunia, C. Fernández-Córdoba, M. Villanueva, *On the linearity and classification on $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes*, Des. Codes Cryptogr. **90**, 1037–1058 (2022). https://doi.org/10.1007/s10623-022-01026-2

[2] C. Carlet, *$\mathbb{Z}_{2^k}$-Linear codes*, IEEE Trans. Inf. Theory **44**(4), 1543–1547 (1998). https://doi.org/10.1109/18.681328

[3] S. T. Dougherty, C. Fernández-Córdoba, *Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes*, Adv. Math. Commun. **5**(4), 571–588 (2011). Doi:10.3934/amc.2011.5.571

[4] S. T. Dougherty, T. A. Gulliver, J. Wong, *Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$*, Des. Codes Cryptogr. **41**, 235–249 (2006). https://doi.org/10.1007/s10623-006-9000-2

[5] H. Eyvazi, K. Samei, B. Savari, *The Homogeneous Gray image of linear codes over the Galois ring $GR(4, m)$*, Cryptogr. Commun. **16**, 531–540 (2023). https://doi.org/10.1007/s12095-023-00683-x

[6] H. Eyvazi, K. Samei, B. Savari, *The linearity of Carlet's Gray image of linear codes over $\mathbb{Z}_8$*, Des. Codes Cryptogr. **90**(10), 2361–2373 (2022). https://doi.org/10.1007/s10623-022-01084-6

[7] C. Fernández-Córdoba, C. Vela, M. Villanueva, *On $\mathbb{Z}_{2^s}$-linear Hadamard codes, kernel and partial classification*, Des. Codes Cryptogr. **87**, 417–435 (2019). https://doi.org/10.1007/s10623-018-0546-6

[8] C. Fernández-Córdoba, C. Vela, M. Villanueva, *On $\mathbb{Z}_8$-linear Hadamard codes, rank and classification*, IEEE Trans. Inf. Theory **66**(2), 970–982 (2020). https://doi.org/10.1109/TIT.2019.2952599

[9] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inf. Theory **40**(2), 301–319 (1994). Doi:10.1109/18.312154

[10] W. C. Huffman, *Decompositions and extremal Type II codes over $\mathbb{Z}_4$*, IEEE Trans. Inf. Theory **44**, 800–809 (1998). Doi:10.1109/18.661525

[11] S. Jitman, P. Udomkavanich, *The Gray image of codes over finite chain rings*, Int. J. Contemp. Math. Sciences **5**(10), 449–458 (2010). https://doi.org/10.48550/arXiv.0907.3397

[12] P. Kanwar, S. R. López-Permouth, *Cyclic codes over the integers modulo p^m*, Finite fields Appl. **3**, 334–352 (1997). Doi:10.1006/ffta.1997.0189

[13] D. S. Krotov, *On $\mathbb{Z}_{2^k}$-dual binary codes*, IEEE Trans. Inf. Theory **53**(4), 1532–1537 (2007). Doi:10.1109/TIT.2007.892787

[14] S. Ling, C. Xing, *Coding theory: a first course*, Cambridge University Press, (2004). https://doi.org/10.1017/CBO9780511755279

[15] J. F. Qain, W. Ma, X. Wang, *On the Gray image of cyclic codes over finite chain rings*, IEICE Tran. Elec. **EA91-A**, 2685–2687 (2008). Doi:10.1093/ietfec/e91-a.9.2685

[16] A. Soufi Karbaski, K. Samei, *Duadic codes over finite local rings*, Bull. Korean Math. Soc. **59** (2), 265-276 (2022). https://doi.org/10.4134/BKMS.b200214

[17] H. Tapia-Recillas, G. Vega, *On $\mathbb{Z}_{2^k}$-linear and quaternary codes*, SIAM J. Discr. Math. **17**(1), 103–113 (2003). https://doi.org/10.1137/S0895480101397219

[18] Z. X. Wan, *Quaternary codes*, World Scientific, Singapore (1997). https://doi.org/10.1142/3603

[19] J. Wolfmann, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inf. Theory **47**(5), 1773–1779 (2001). Doi:10.1016/S1571-0653(04)00179-9

Department of Mathematics, Faculty of Science, Bu Ali Sina University, Hamedan, Iran.

E-mail address: *a.mehri@sci.basu.ac.ir*

E-mail address: *h.eyvazi@sci.basu.ac.ir*

E-mail address: *samei@basu.ac.ir*, *samei@ipm.ir*

The linearity of the Homogeneous Gray image of linear codes over $\mathbb{Z}_9$

Alireza Mehry(1), **Hamidreza Eyvazi**(1) **and Karim Samei**(1)†

(1) Department of Mathematics, Faculty of Science, Bu Ali Sina University, Hamedan, Iran

Communicated by:

Received: Accepted:

Abstract: The $\mathbb{Z}_9$-additive codes of length n are subgroups of $\mathbb{Z}_9^n$. Let $\mathcal{C}$ be a linear code of length n over $\mathbb{Z}_9$ and Φ be the Homogeneous Gray map on $\mathbb{Z}_9^n$. In this paper, we show that $\Phi(\mathcal{C})$ is linear if and only if for every $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$, $(\boldsymbol{u} \circledast \boldsymbol{v}) \in \mathcal{C}$. When $\mathcal{C}$ is cyclic and n is relatively prime to 3, using the generator polynomial a necessary and sufficient condition is given for linearity its homogeneous Gray image. As a result, it is shown that the Homogeneous Gray image of a quadratic residue code over $\mathbb{Z}_9$ is not linear.

Keywords: Cyclic code, Homogeneous Gray map, Linear code, Mattson-Solomon transform.

Mathematics Subject Classification: 94B15, 11T71.

---

† Corresponding author E-mail address: samei@basu.ac.ir