

## تصویر گری کدهای ثابت‌دوری روی برخی از حلقه‌های چندجمله‌ای خارج‌قسمتی

رضا سبحانی

دانشگاه اصفهان، گروه ریاضی

پذیرش ۹۸/۰۶/۱۰

دریافت ۹۶/۱۲/۱۳

### چکیده

فرض کنید  $R_S$  حلقهٔ خارج‌قسمتی  $F_{p^m}[u]/\langle u^s \rangle$  باشد که در آن  $F_{p^m}$  میدان متناهی از اندازه  $p^m$  و  $s$  یک عدد صحیح مثبت است. یک تابع گری  $\Phi$  به طول  $l$  روی  $R_S$  یک نگاشت خاص از  $R_S$  به  $(F_{p^m})^l$  است. تابع گری  $\Phi$  را  $(\lambda, \theta)$ -تابع گوییم هرگاه تصویر هر کد  $\lambda$ -ثابت‌دوری روی  $R_S$  یک کد  $\theta$ -ثابت‌دوری روی میدان  $F_{p^m}$  باشد. در این مقاله به بررسی وجود  $(\lambda, \theta)$ -تابع‌های گری روی  $R_S$  می‌پردازیم. در این راستا، یک شرط معادل برای چنین توابعی می‌یابیم. سپس ثابت می‌کنیم که اگر  $\Phi$  یک  $(\lambda, \theta)$ -تابع گری به طول  $l$  روی  $R_S$  باشد و  $\lambda = \lambda_0 + \lambda_1 u + \dots + \lambda_{s-1} u^{s-1}$  و آن‌گاه  $\theta = \lambda_0^l$ ،  $\lambda_1 \neq 0$  و  $p$  طول تابع گری یعنی  $l$  را می‌شمارد. هم چنین ثابت می‌کنیم، اگر  $\theta = 1$  آن‌گاه  $\lambda_0 = 1$  علاوه‌براین، تمامی چنین توابعی را روی  $R_2$  محاسبه می‌کنیم. در پایان یک  $(\lambda, \lambda_0^{p^k})$ -تابع گری به طول  $p^k$  روی  $R_S$  معرفی می‌کنیم که  $p^{k-1} < s \leq p^k$ .

واژه‌های کلیدی: تابع گری، کد ثابت‌دوری، حلقهٔ زنجیری، حلقهٔ باقی‌ماندهٔ چندجمله‌ای.

### مقدمه

منظور از یک کد  $C$  به طول  $n$  روی حلقهٔ  $R$ ، یک زیرمجموعه از  $R^n$  است. کد  $C$  را یک کد خطی گوییم هرگاه  $R$ -زیرمدول  $R^n$  باشد. به حلقهٔ  $R$  الفبای کد گوییم. کد  $C$  را  $\alpha$ -ثابت دوری گوییم هرگاه  $(c_0, c_1, \dots, c_{n-1}) \in C$  نتیجه دهد  $(\alpha c_{n-1}, c_0, \dots, c_{n-2}) \in C$ . درحالتی که  $\alpha = 1$ ، کد را دوری<sup>۱</sup> و در حالتی که داشته باشیم  $\alpha = -1$ ، کد را منفی‌دوری<sup>۲</sup> گوییم. در نظریه کلاسیک کدگذاری، الفبای کدها میدان متناهی در نظر گرفته می‌شد. بعد از این‌که نویسندگان در [۴]، توانستند دستهٔ مهمی از کدهای غیرخطی دودویی را از تصویر گری<sup>۳</sup> کدهای دوری توسعه‌یافته روی حلقهٔ  $Z_4$  به‌دست آورند، علاقهٔ محققان به بررسی کدها روی حلقه‌های متناهی و هم‌چنین توابع گری، به‌عنوان مرتبط‌کنندهٔ کدها روی حلقه‌های متناهی، به کدها روی میدان‌های متناهی، افزایش یافت. ولگمن [۱۲]، ثابت کرد که تصویر گری یک کد منفی‌دوری روی  $Z_4$ ، یک کد دوری دودویی است. این کار زمینهٔ تحقیق در ارتباط کدهای ثابت‌دوری<sup>۴</sup> روی حلقه‌ها و کدهای ثابت‌دوری روی میدان‌ها را فراهم آورد. در ادامه، با ارائهٔ تعمیمی از تابع گری، نتایج [۱۲] به کدهای ثابت‌دوری خاصی روی حلقهٔ  $Z_{p^m}$  تعمیم داده شد، [۶] را ببینید. با معرفی یک تابع گری برای حلقهٔ  $F_2 + uF_2$ ، در [۸] ثابت شد که تصویر گری هر کد  $(1+u)$ -ثابت‌دوری روی  $F_2 + uF_2$ ، یک کد دوری روی  $F_2$  است. تعمیم‌هایی نیز برای این حلقه در مقالات [۱]، [۲]، [۵]،

\*نویسنده مسئول r.sobhani@sci.ui.ac.ir

1. Cyclic  
2. Negacyclic  
3. Gray  
4. Constacyclic

[۸]، [۹] و [۱۱] به دست آمده است. نویسنده در [۱۰] یک تابع گری برای یک گروه متناهی را تعریف و به بررسی وجود توابع مختلف گری روی یک  $p$ -گروه متناهی پرداخته است.

در اغلب مقالات ذکر شده، توابع گری خاصی مطرح شده‌اند و تصدیق شده است که تابع گری معرفی شده، خاصیت انتقال دسته‌ای از کدهای ثابت‌دوری روی حلقه موردنظر را به دسته خاصی از کدها روی میدان متناهی، داراست. مثلاً در کار ولفمن ثابت شد که تابع گری شناخته شده روی  $Z_4$ ، هر کد منفی‌دوری روی  $Z_4$  را به یک کد دوری روی  $Z_4$  انتقال می‌دهد. تا کنون هیچ کار تحقیقاتی روی دسته‌بندی تمامی توابع گری که کدهای ثابت‌دوری روی یک حلقه مشخص را به کدهای ثابت‌دوری روی یک میدان متناهی منتقل می‌کنند، انجام نشده است. در این مقاله با در نظر گرفتن حلقه  $R_S = \frac{F_p^m[u]}{\langle u^s \rangle}$  و تعریف یک  $(\lambda, \theta)$ -تابع گری، به عنوان تابعی که هر کد  $\lambda$ -ثابت‌دوری روی  $R_S$  را به کد  $\theta$ -ثابت‌دوری روی  $F_p^m$  منتقل می‌کند، قصد داریم تا با ارائه یک شرط لازم و کافی برای  $(\lambda, \theta)$ -تابع‌های گری روی  $R_S$ ، به دسته‌بندی آنها پرداخته و روی شرایط وجود آنها بحث کنیم. در این راستا، ثابت می‌کنیم که اگر  $\Phi$  یک  $(\lambda, \theta)$ -تابع گری به طول  $l$  روی  $R_S$  باشد و  $\lambda = \lambda_0 + \lambda_1 u + \dots + \lambda_{s-1} u^{s-1}$  و  $\theta = \lambda_0^l$  و  $p$  طول  $\Phi$  یعنی  $l$  را می‌شمارد. هم‌چنین ثابت می‌کنیم که اگر  $\theta = 1$  آن‌گاه  $\lambda_0 = 1$  علاوه بر این، تمامی چنین توابعی را روی  $R_2$  محاسبه می‌کنیم. در پایان یک  $(\lambda, \lambda_0^{p^k})$ -تابع گری روی  $R_S$  معرفی می‌کنیم که در آن  $\lambda$  عضو وارون‌پذیر دل‌خواهی از  $R_S$  است.

### برخی پیش‌نیازها: کدهای ثابت‌دوری و حلقه $R_S$

در این بخش کدهای ثابت‌دوری روی یک حلقه دل‌خواه را معرفی کرده و سپس به معرفی حلقه  $R_S$  می‌پردازیم. در ادامه برخی خواص این حلقه را یادآوری می‌کنیم.

**تعریف ۱.** فرض کنید  $R$  یک حلقه متناهی دل‌خواه باشد. یک کد  $C$  به طول  $n$  روی  $R$ ، یک زیرمجموعه  $R^n$  است. کد  $C$  را خطی گوئیم هرگاه  $R$ -زیرمدول  $R^n$  باشد.

**تعریف ۲.** فرض کنید  $C$  یک کد خطی به طول  $n$  روی  $R$  است و  $\alpha$  یک عضو وارون‌پذیر از  $R$  باشد. کد  $C$  را  $\alpha$ -ثابت دوری گوئیم هرگاه  $(c_0, c_1, \dots, c_{n-1}) \in C$  نتیجه دهد  $(\alpha c_{n-1}, c_0, \dots, c_{n-2}) \in C$ . در حالتی که  $\alpha = 1$ ، کد را دوری و در حالتی که  $\alpha = -1$ ، کد را منفی‌دوری گوئیم.

**تعریف ۳.** فرض کنید  $p$  یک عدد اول و  $m, s$  دو عدد طبیعی باشند. هم‌چنین فرض کنید  $F_p^m$  میدان متناهی از مرتبه  $p^m$  است و  $F_p^m[u]$  نمایان‌گر حلقه چندجمله‌ای‌ها روی  $F_p^m$  با متغیر  $u$  باشد. حلقه  $R_S$  را برابر حلقه خارج‌قسمتی

$$R_S := \frac{F_p^m[u]}{\langle u^s \rangle}$$

تعریف می‌کنیم.

مشخص است که حلقه  $R_S$  یک حلقه جابه‌جایی و یک‌دار متناهی از اندازه  $p^{ms}$  است. از طرفی، بنابر قضیه XVII.5 از [۷]،  $R_S$  یک حلقه زنجیری و لذا یک حلقه موضعی با ایده‌ال ماکزیمال  $\langle u \rangle$  است. هر عنصر  $r$  متعلق به  $R_S$  را می‌توان به صورت  $r = r_0 + r_1 u + \dots + r_{s-1} u^{s-1}$  نوشت که  $r_i \in F_p^m$  چون در یک حلقه موضعی، مجموعه عناصر خارج از ایده‌ال ماکزیمال برابر مجموعه عناصر وارون‌پذیر حلقه است، عضو  $r$  وارون‌پذیر است اگر و تنها اگر  $r_0 \neq 0$

### تابع گری روی $R_S$ و $(\lambda, \theta)$ -تابع گری

در این بخش به تعریف تابع گری روی  $R_S$  پرداخته و  $(\lambda, \theta)$ -تابع گری را نیز تعریف می‌کنیم. در ادامه بخش، شرایط معادلی را برای این که یک تابع  $\Phi$  یک  $(\lambda, \theta)$ -تابع گری باشد بیان و اثبات می‌کنیم.

**تعریف ۴.** منظور از یک تابع گری  $\phi$  به طول  $l$  روی  $R_S$  یک ماتریس  $S \times l$  با بعد  $S$  روی  $F_p^m$  است. برای عضو  $r$  متعلق به  $R_S$  که  $r = r_0 + r_1u + \dots + r_{s-1}u^{s-1}$  تصویر گری  $r$  را برابر با حاصلضرب بردار  $[r_0, r_1, \dots, r_{s-1}]$  در ماتریس  $\phi$  تعریف می‌کنیم. یعنی  $\phi(r) = [r_0, r_1, \dots, r_{s-1}]\phi$ . در این حالت می‌نویسیم:  $\phi(r) = (\phi_0(r), \phi_1(r), \dots, \phi_{l-1}(r))$ . همچنین برای بردار  $v = (v_0, v_1, \dots, v_{N-1})$  در  $R_S^N$  می‌نویسیم

$$\begin{aligned}\phi(v) &= (\phi_0(v_0), \phi_0(v_1), \dots, \phi_0(v_{N-1}), \\ &\quad \phi_1(v_0), \phi_1(v_1), \dots, \phi_1(v_{N-1}), \\ &\quad \phi_{l-1}(v_0), \phi_{l-1}(v_1), \dots, \phi_{l-1}(v_{N-1})).\end{aligned}$$

**تعریف ۵.** فرض کنید  $\lambda$  عضو وارون‌پذیری از  $R_S$  و  $\theta$  عضو وارون‌پذیری از  $F_p^m$  باشند. تابع گری  $\phi$  را یک  $(\lambda, \theta)$ -تابع گری گوئیم هرگاه تصویر هر کد  $\lambda$ -ثابت دوری روی  $R_S$  به وسیله  $\phi$  یک کد  $\theta$ -ثابت دوری روی  $F_p^m$  باشد.

**تعریف ۶.** فرض کنید  $R$  یک حلقه و  $\lambda$  عضو وارون‌پذیری از  $R$  باشد. جایگشت  $\sigma_\lambda$  روی  $R^N$  را به صورت

$$\sigma_\lambda(v_0, v_1, \dots, v_{N-1}) = (\lambda v_{N-1}, v_0, \dots, v_{N-2})$$

تعریف می‌کنیم.

**قضیه ۷.** شرایط زیر معادل‌اند:

(الف)  $\phi$  یک  $(\lambda, \theta)$ -تابع گری روی  $R_S$  است.

(ب) برای هر  $a \in R_S$  داریم  $\phi(\lambda a) = \sigma_\theta(\phi(a))$ .

(ج) برای هر عدد طبیعی  $N$  و هر بردار  $v = (v_0, v_1, \dots, v_{N-1})$  در  $R_S^N$  داریم  $\phi(\sigma_\lambda(v)) = \sigma_\theta(\phi(v))$ .  
**اثبات:** از (ب) به (ج) و از (ج) به (الف) بدیهی است. تنها (الف) به (ب) را اثبات می‌کنیم. فرض کنید  $\phi$  یک  $(\lambda, \theta)$ -تابع گری روی  $R_S$  است و  $a \in R_S$ . اکنون عدد طبیعی  $N \geq 2$  را طوری در نظر می‌گیریم که  $\gcd(N, p) = 1$

بنابر لم XV.1 از [7]، عضو  $\delta$  در  $R_S$  موجود است که  $\delta^N = \lambda$ . حال قرار دهید

$$C := \langle (\delta^{N-1}, \delta^{N-2}, \dots, \delta, 1) \rangle.$$

یعنی  $C$  همان  $R_S$ -زیرمدول دوری تولید شده به وسیله  $(\delta^{N-1}, \delta^{N-2}, \dots, \delta, 1)$  از  $R_S$ -مدول  $R_S^N$  است. می‌توان دید که  $C$  یک کد  $\lambda$ -ثابت دوری است. چون  $\phi$  یک  $(\lambda, \theta)$ -تابع گری است باید برای یک  $b \in R_S$  داشته باشیم

$$\sigma_\theta \left( \phi \left( (a\delta^{N-1}, a\delta^{N-2}, \dots, a\delta, a) \right) \right) = \phi \left( (b\delta^{N-1}, b\delta^{N-2}, \dots, b\delta, b) \right).$$

به عبارت دیگر باید داشته باشیم

$$\begin{aligned}(\phi_0(b\delta^{N-1}), \phi_0(b\delta^{N-2}), \dots, \phi_0(b), \\ \phi_1(b\delta^{N-1}), \phi_1(b\delta^{N-2}), \dots, \phi_1(b), \\ \phi_{l-1}(b\delta^{N-1}), \phi_{l-1}(b\delta^{N-2}), \dots, \phi_{l-1}(b)) = \\ (\phi_{l-1}(a), \phi_0(a\delta^{N-1}), \dots, \phi_0(a\delta), \\ \phi_0(a), \phi_1(a\delta^{N-1}), \dots, \phi_1(a\delta))\end{aligned}$$

$$\phi_{1-2}(a), \phi_{1-1}(a\delta^{N-1}), \dots, \phi_{1-1}(a\delta)$$

با توجه به یک به یک بودن  $\phi$  و این که  $N \geq 2$  داریم  $a\delta^{N-1} = b\delta^{N-2}$  و در نتیجه  $b = a\delta$ . هم‌چنین داریم:

$$\sigma_\theta(\phi(a)) = \phi(b\delta^{N-1}) = \phi(a\delta\delta^{N-1}) = \phi(a\lambda).$$

با توجه به دل‌خواه بودن  $a$ ، حکم ثابت است.

اکنون فرض کنید  $r = r_0 + r_1u + \dots + r_{s-1}u^{s-1}$  عضو  $R_s$  باشد و قرار دهید

$$M_r = \begin{pmatrix} r_0 & r_1 & \dots & r_{s-2} & r_{s-1} \\ 0 & r_0 & \dots & r_{s-3} & r_{s-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & r_0 \end{pmatrix}.$$

به‌علاوه قرار دهید

$$S_s := \{M_r \mid r \in R_s\}.$$

به‌وضوح  $S_s$  یک زیرحلقه از حلقه ماتریس‌های  $s \times s$  روی  $F_{p^m}$  است و داریم  $S_s \cong R_s$  برای  $\theta \in F_{p^m}$  قرار

می‌دهیم

$$D_\theta := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \theta & 0 & 0 & \dots & 0 \end{pmatrix}$$

حال شرط دوم از قضیه قبل معادل است با این که

$$M_\lambda \phi = \phi D_\theta. \tag{۱}$$

فرض کنید

$$\phi = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,l-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{s-1,0} & g_{s-1,1} & \dots & g_{s-1,l-1} \end{pmatrix}.$$

اگر بنویسیم  $\lambda = \lambda_0 + \lambda_1u + \dots + \lambda_{s-1}u^{s-1}$  آن‌گاه معادله (۱) معادل است با

$$\begin{pmatrix} \lambda_0 & \lambda_1 & \dots & \lambda_{s-2} & \lambda_{s-1} \\ 0 & \lambda_0 & \dots & \lambda_{s-3} & \lambda_{s-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \lambda_0 \end{pmatrix} \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,l-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{s-1,0} & g_{s-1,1} & \dots & g_{s-1,l-1} \end{pmatrix} = \begin{pmatrix} \theta g_{0,l-1} & g_{0,0} & \dots & g_{0,l-2} \\ \theta g_{1,l-1} & g_{1,0} & \dots & g_{1,l-2} \\ \vdots & \vdots & \ddots & \vdots \\ \theta g_{s-1,l-1} & g_{s-1,0} & \dots & g_{s-1,l-2} \end{pmatrix}. \tag{۲}$$

قضیه ۸. اگر  $\phi$  یک  $(\lambda, \theta)$ -تابع گری به طول  $l$  روی  $R_s$  باشد آن‌گاه  $\lambda_0^l = \theta$  و عضو غیر صفر  $\delta$  در  $F_{p^m}$  موجود

است که سطر  $s$ ام ماتریس  $\phi$  برابر خواهد بود با  $(\lambda_0^{l-1}\delta, \lambda_0^{l-2}\delta, \dots, \delta)$ . هم‌چنین اگر  $\theta = 1$  آن‌گاه داریم

$$\lambda_0 = 1$$

**اثبات:** با برابر قرار دادن سطرهای  $s$  ام از ماتریس‌های رابطه (۲) داریم  $\theta g_{s-1,l-1} = \lambda_0 g_{s-1,0}$  و همچنین برای هر  $i$  که  $1 \leq i \leq s-1$  داریم:

بنابراین می‌توان نتیجه گرفت که  $\theta g_{s-1,l-1} = g_{s-1,l-1} \lambda_0^l$ . اکنون اگر  $g_{s-1,l-1} = 0$  آن‌گاه سطر  $s$  ام ماتریس  $\phi$  برابر صفر میشود که در تناقض با رتبه کامل بودن  $\phi$  است. پس داریم  $\lambda_0^l = \theta$  و با قرار دادن  $\delta = g_{s-1,l-1}$ :  
حکم ثابت است. اکنون اگر  $\theta = 1$  آن‌گاه باید داشته باشیم  $\lambda_0^l = 1$  چون  $\lambda_0$  عضوی از گروه ضربی میدان  $F_{p^m}$  است پس باید مرتبه  $\lambda_0$  شمارنده‌ای از  $p^m - 1$  باشد. اما  $l$  مضربی از  $p$  است و داریم  $\gcd(p, p^m - 1) = 1$  پس باید داشته باشیم  $\lambda_0 = 1$

**قضیه ۹.** اگر  $\phi$  یک  $(\lambda, \theta)$ -تابع گری به طول  $l$  روی  $R_s$  باشد آن‌گاه باید داشته باشیم  $\lambda_1 \neq 0$  و  $p|l$  همچنین عضو  $\gamma$  در  $F_{p^m}$  موجود است که سطر  $(s-1)$  ام ماتریس  $\phi$  برابر است با

$$(\lambda_0^{l-1} \gamma + (1-1)\lambda_0^{l-2} \lambda_1 \delta, \dots, \lambda_0 \gamma + \lambda_1 \delta, \gamma).$$

**اثبات:** با برابر قرار دادن سطرهای  $(s-1)$  ام ماتریس‌های رابطه (۲) داریم:

$$\lambda_0 g_{s-2,0} + \lambda_1 g_{s-1,0} = \theta g_{s-2,l-1},$$

و برای  $0 \leq i \leq l-2$  داریم

$$\lambda_0 g_{s-2,i+1} + \lambda_1 g_{s-1,i+1} = g_{s-2,i}.$$

با توجه به این که سطر  $s$  ام ماتریس  $\phi$  برابر است با  $(\lambda_0^{l-1} \delta, \lambda_0^{l-2} \delta, \dots, \delta)$  و  $\lambda_0^l = \theta$  داریم

$$\lambda_0 g_{s-2,0} + \lambda_1 \lambda_0^{l-1} \delta = \lambda_0^l g_{s-2,l-1},$$

و برای  $0 \leq i \leq l-2$  داریم

$$\lambda_0 g_{s-2,i+1} + \lambda_1 \lambda_0^{l-2-i} \delta = g_{s-2,i}.$$

بنابراین، با ضرب کردن در توان مناسبی از  $\lambda_0$  داریم

$$\lambda_0 g_{s-2,0} - \lambda_0^l g_{s-2,l-1} = -\lambda_1 \lambda_0^{l-1} \delta,$$

$$\lambda_0^2 g_{s-2,1} - \lambda_0 g_{s-2,0} = -\lambda_1 \lambda_0^{l-1} \delta,$$

$$\lambda_0^l g_{s-2,l-1} - \lambda_0^{l-1} g_{s-2,l-2} = -\lambda_1 \lambda_0^{l-1} \delta.$$

با جمع زدن طرفین روابط بالا داریم  $-l\lambda_1 \lambda_0^{l-1} \delta = 0$ . اما  $\lambda_0$  و  $\delta$  غیر صفر هستند. اگر  $\lambda_1 = 0$  و همچنین  $g_{s-2,l-1} = 0$  آن‌گاه سطر  $(s-1)$  ام ماتریس  $\phi$  برابر صفر می‌شود و اگر  $\lambda_1 = 0$  و  $g_{s-2,l-1} \neq 0$  عضو غیر صفری مانند  $\gamma$  باشد آن‌گاه سطر  $(s-1)$  ام ماتریس  $\phi$  برابر مضربی از سطر  $s$  ام آن می‌شود که در هر دو صورت با رتبه کامل بودن  $\phi$  در تناقض است. از این رو داریم  $\lambda_1 \neq 0$  و همچنین  $g_{s-2,l-1}$  عضو غیر صفری مانند  $\gamma$  است. حال می‌توان از  $-l\lambda_1 \lambda_0^{l-1} \delta = 0$  نتیجه گرفت که  $l = 0$  و این یعنی مشخصه میدان یا همان  $p$ ، طول تابع گری یا همان  $l$  را می‌شمارد. به علاوه سطر  $(s-1)$  ام ماتریس  $\phi$  نیز چنان‌که ادعا شده بود، به دست می‌آید.

در [۳] وارون پذیرهای  $R_s$  به انواع مختلف دسته‌بندی شده‌اند. در واقع  $\lambda = \lambda_0 + \lambda_1 u + \dots + \lambda_{s-1} u^{s-1}$  را که  $\lambda_0 \neq 0$  از نوع  $t$  گوئیم هرگاه  $t$  کوچک‌ترین عددی بین  $1$  تا  $s-1$  باشد که  $\lambda_t \neq 0$  هم‌چنین یادآوری می‌کنیم که کدهای ثابت دوری به طول  $N$  را که  $p|N$ ، کد ثابت دوری با ریشه تکراری گوئیم. اکنون اگر  $\phi$  یک  $(\lambda, \theta)$ -تابع گری به طول  $l$  روی  $R_s$  باشد، از قضیه ۹ داریم  $\lambda_1 \neq 0$  و از این رو  $\lambda$  باید از نوع ۱ باشد. به علاوه، از

$p|l$  نتیجه می‌شود که طول کدهای ثابت‌دوری بدست آمده توسط تابع گری، مضرب  $p$  است و بنابراین چنین کدهایی، با ریشه تکراری هستند. مطالب بالا در نتیجه زیر جمع‌بندی شده است.

نتیجه ۱۰. اگر  $\lambda$  از نوع  $t$  باشد که  $t \geq 2$ ، آن‌گاه هیچ  $(\lambda, \theta)$ -تابع گری روی  $R_S$  موجود نیست. به‌علاوه همه کدهای به‌دست آمده از تصویر کدهای ثابت‌دوری روی  $R_S$  به‌وسیله یک  $(\lambda, \theta)$ -تابع گری، کدهای ثابت‌دوری با ریشه تکراری هستند.

در نتیجه ۱۱، تمام  $(\lambda, \theta)$ -توابع گری روی  $R_2$  را رده‌بندی می‌کنیم. اثبات آن از قضیه ۹ نتیجه می‌شود.

نتیجه ۱۱. هر  $(\lambda, \theta)$ -تابع گری  $\phi$  با طول  $l = pl'$  روی  $R_2$  بدین صورت است:

$$\phi = \left[ \lambda_0^{(l'-1)p} \phi' \mid \dots \mid \lambda_0^p \phi' \mid \phi' \right]$$

که در آن

$$\phi' = \begin{pmatrix} \lambda_0^{p-1} \gamma + (p-1)\lambda_0^{p-2} \lambda_1 \delta & \dots & \lambda_0 \gamma + \lambda_1 \delta & \gamma \\ \lambda_0^{p-1} \delta & \dots & \lambda_0 \delta & \delta \end{pmatrix}.$$

مثال ۱۲. در این مثال، تمامی  $(1 + 2u, 1)$ -توابع گری به‌طول ۳ روی  $\frac{F_3[u]}{\langle u^2 \rangle}$  را محاسبه می‌کنیم. با نمادهای نتیجه ۱۱، داریم  $\lambda_0 = 1$ ،  $\lambda_1 = 2$ ،  $l' = 1$  و  $p = 3$  هم‌چنین،  $\delta$  و  $\gamma$  دو عضو غیرصفر از  $F_3$  هستند. از این رو چهار حالت رخ می‌دهد. در حالت اول داریم  $\delta = \gamma = 1$  و بنابراین

$$\phi_1 = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

در حالت دوم داریم  $\delta = 2$ ،  $\gamma = 1$  و بنابراین

$$\phi_2 = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix}.$$

در حالت سوم داریم  $\delta = 1$ ،  $\gamma = 2$  و بنابراین

$$\phi_3 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

در حالت چهارم داریم  $\delta = 2$ ،  $\gamma = 2$  و بنابراین

$$\phi_4 = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 2 & 2 \end{pmatrix}.$$

از این رو  $\phi_1$ ،  $\phi_2$ ،  $\phi_3$  و  $\phi_4$  تمامی  $(1 + 2u, 1)$ -توابع گری به‌طول ۳ روی  $\frac{F_3[u]}{\langle u^2 \rangle}$  هستند.

گرچه برای  $S = 2$ ، فرم کلی تمام  $(\lambda, \theta)$ -توابع گری را به‌دست آوردیم و هم‌چنین شرایط لازم خوبی را برای وجود این توابع به‌دست آوردیم ولی با چنین تحلیلی، به‌سختی می‌توان یک  $(\lambda, \theta)$ -تابع گری برای  $R_S$  در حالت کلی ساخت. در واقع دقت کنید که حتی می‌توانیم یک  $(\lambda, \theta)$ -تابع گری روی  $R_S$  را که  $\lambda = \lambda_0 + \lambda_1 u + \dots + \lambda_{s-1} u^{s-1}$  به یک  $(\lambda', \theta)$ -تابع گری روی  $R_{S+1}$  گسترش دهیم که  $\lambda' = \lambda + \lambda_s u^s$  راه حل این کار ساده است و نیازی به بیان آن نیست، مهم این است که این روند را نمی‌توان برای یافتن یک  $(\lambda, \theta)$ -تابع گری برای  $R_S$  در حالت کلی، به کار برد.

در حالت خاص می‌توانیم با روش دیگری به حل چنین مسئله‌ای بپردازیم. در بخش بعد، وقتی که  $S = p^k$  توانی از عدد اول  $p$  است، یک  $(\lambda, \theta)$ -تابع گری به‌طول  $S$  روی  $R_S$  می‌سازیم.

نکته ۱۳. بدیهی است که اگر  $\phi$  یک  $(\lambda, \theta)$ -تابع گری به‌طول  $S$  روی  $R_S$  باشد و هم‌چنین  $1 \leq t \leq S$ ، آن‌گاه  $\phi_t$

که متشکل از  $t$  سطر آخر  $\phi$  است، یک  $(\lambda, \theta)$ -تابع گری به‌طول  $S$  روی  $R_t$  است که در آن

$$\bar{\lambda} = \lambda_0 + \lambda_1 u + \dots + \lambda_{t-1} u^{t-1} = \lambda \pmod{u^t}.$$

### یک $(\lambda, \theta)$ -تابع گری به طول $p^k$ روی $R_{p^k}$

در این بخش قرار می‌دهیم  $s := p^k$  و یک  $(\lambda, \theta)$ -تابع گری به طول  $s$  روی  $R_s$  می‌سازیم. ابتدا دقت کنید که اگر

$$\lambda = \lambda_0 + \lambda_1 u + \dots + \lambda_{s-1} u^{s-1}$$

آن‌گاه  $\lambda_0, \lambda_1 \neq 0$  از این‌رو می‌توانیم بنویسیم  $\lambda = \lambda_0 + \alpha u$  که در آن  $\alpha = \lambda_1 + \lambda_2 u + \dots + \lambda_{s-1} u^{s-2}$  عضو وارون‌پذیری از  $R_s$  است. بدیهی است که  $R_s$  یک فضای برداری با بعد  $s$  روی  $F_{p^m}$  است که  $A = \{1, u, u^2, \dots, u^{s-1}\}$  یک پایه برای آن است. لم ۱۴ هم دارای اثبات ساده‌ای است که از بیان آن صرف‌نظر می‌کنیم.

لم ۱۴. در  $R_s$  داریم  $\lambda^s = \lambda_0^s \in F_{p^m}$  و مجموعه  $B = \{1, \lambda, \lambda^2, \dots, \lambda^{s-1}\}$  نیز یک پایه برای فضای برداری  $R_s$  روی  $F_{p^m}$  است.

اکنون متناظر با پایه‌های  $A$  و  $B$  یک ماتریس تبدیل پایه  $G_{A,B}$  موجود است که اگر  $r = r_0 + r_1 u + \dots + r_{s-1} u^{s-1}$

$$[r_0, r_1, \dots, r_{s-1}] G_{A,B} = [a_0, a_1, \dots, a_{s-1}]$$

$$r = a_0 + a_1 \lambda + \dots + a_{s-1} \lambda^{s-1}$$

آن‌گاه داریم قضیه ۱۵.  $G_{A,B}$  یک  $(\lambda, \lambda_0^s)$ -تابع گری به طول  $s$  روی  $R_s$  است.

اثبات: قرار دهید  $\phi := G_{A,B}$  و  $\theta := \lambda_0^s$ . برای هر  $r = r_0 + r_1 u + \dots + r_{s-1} u^{s-1}$  در  $R_s$  نشان می‌دهیم

$$\phi(\lambda r) = \sigma_\theta(\phi(r)).$$

فرض کنید  $\phi(r) = [a_0, a_1, \dots, a_{s-1}]$  پس  $\phi(r) = a_0 + a_1 \lambda + \dots + a_{s-1} \lambda^{s-1}$  از طرفی چون  $\lambda r = \theta a_{s-1} + a_0 \lambda + \dots + a_{s-2} \lambda^{s-2}$  بنابراین  $\lambda^s = \lambda_0^s = \theta$

$$\phi(\lambda r) = [\theta a_{s-1}, a_0, \dots, a_{s-2}] = \sigma_\theta(\phi(r))$$

و اثبات تمام است.

اکنون با توجه به نکته قبل، برای هر  $t$  که  $p^{k-1} < t \leq p^k$  می‌توان یک تابع گری به طول  $s$  روی  $R_t$  ساخت. حال ممکن است محاسبه دقیق ماتریس  $G_{A,B}$  در بالا، کار چندان راحتی نباشد اما به هر حال وجود چنین توابعی به اثبات رسید. اکنون در یک حالت خاص، فرض کنید  $\lambda = \lambda_0 + u$  می‌خواهیم در این حالت  $G_{A,B}$  را دقیق محاسبه کنیم. برای هر  $0 \leq i \leq s-1$  داریم

$$\lambda^i = \sum_{j=0}^{i-1} \binom{i}{j} \lambda_0^{i-j} u^j$$

بنابراین اگر  $r = a_0 + a_1 \lambda + \dots + a_{s-1} \lambda^{s-1}$  آن‌گاه  $r = r_0 + r_1 u + \dots + r_{s-1} u^{s-1}$  که در آن

$$[r_0, r_1, \dots, r_{s-1}] = [a_0, a_1, \dots, a_{s-1}] H_\lambda$$

و  $H_\lambda$  ماتریسی است که درایه  $(i, j)$  آن برابر  $\binom{i}{j} \lambda_0^{i-j}$  است. اکنون می‌توان دید که ماتریس  $G_\lambda$  که درایه  $(i, j)$

آن برابر  $\binom{i}{j} \lambda_0^{i-j} (-1)^{i+j}$  است، وارون ماتریس  $H_\lambda$  است و از این‌رو داریم

$$[r_0, r_1, \dots, r_{s-1}] G_\lambda = [a_0, a_1, \dots, a_{s-1}].$$

پس ماتریس  $\phi = G_\lambda$  یک  $(\lambda, \lambda_0^s)$ -تابع گری به طول  $s$  روی  $R_s$  است.

### تقدیر و تشکر

از داوران محترم که مقاله را با دقت بررسی و ارزیابی کردند و با نظرات ارزشمند خود به بهبود این مقاله کمک کرده‌اند، کمال سپاس و قدردانی خود را اعلام می‌داریم.

### منابع

1. Cao Yuan, Cao Yonglin, "The Gray image of constacyclic codes over the finite chain ring  $F_p^m[u]\langle u^k \rangle$ ", J. Appl. Math. Comput., 57 (2018) 303-320.
2. Ding J., Li H., "The Gray image of a class of constacyclic codes over polynomial residue rings, J. Franklin Inst., 351 (2014) 5467-5479.
3. Dinh H. Q., Dhompongsab S., Sriboonchitta S., "Repeated-root constacyclic codes of prime power length over  $F_p^m[u]/\langle u^a \rangle$  and their duals", Discrete Math., 339 (2016) 1706-1715.
4. Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Sole P., "The  $Z_4$ -linearity of Kerdock, Preparata, Goethals, and related codes", IEEE Trans. Inform. Theory, 40 (1994) 301-319.
5. Jitman S., Udomkavanich P., "The Gray image of codes over finite chain rings", Int. J. Contemp. Math. Sciences, 5 (2010) 449-458.
6. Ling S., Blackford T., " $Z_{p^{k+1}}$ -linear codes", IEEE Trans. Inform. Theory, 48 (2002) 2592-2605.
7. McDonald B. R., "Finite Rings With Identity", Marcel Dekker Incorporated, New York, 1974.
8. Qian J. F., Zhang L. N., Zhu S. X., " $(1+u)$ -Constacyclic and cyclic codes over  $F_2 + uF_2$ ", Appl. Math. Lett., 19 (2003) 820-823.
9. Qian J. F., Zhang L. N., Zhu S. X., "Constacyclic and cyclic codes over  $F_2 + uF_2 + u^2F_2$ ", IEICE Trans. Fundamentals, E89-A (2006) 1863-1865.
10. Sobhani R., "Gray isometries for finite p-groups", Trans. Comb., 2 (2013) 17-26.
11. Sobhani R., Esmaeili M., "Some constacyclic and cyclic codes over  $F_q[u]\langle u^{t+1} \rangle$ ", IEICE Trans. Fundamentals, E93-A (2010) 808-813.
12. Wolfman J., "Negacyclic and cyclic codes over  $Z_4$ ", IEEE Trans. Inform. Theory, 45 (1999) 2527-2532.
13. Zhu S. X., Wu B., "Gray images of linear codes and constacyclic codes over the ring  $F_p + uF_p + \dots + u^kF_p$ ", J. Hefei Univ. Technol. Nat. Sci., 29 (2006) 1049-1052.