تصویر گری کدهای ثابت‌دوری روی برخی از حلقه‌های چندجمله‌ای خارج‌قسمتی

رضا سبحانی
دانشگاه اصفهان، گروه ریاضی

دریافت ۹۶/۱۲/۱۳ پذیرش ۹۸/۰۶/۱۰

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 اندازهٔ p^m و s یک عدد صحیح مثبت است. یک تابع گری Φ به‌طول l روی R_s یک نگاشت خاص از R_s به $(F_{p^m})^l$ است. تابع گری Φ را (λ,θ)- تابع گوییم هرگاه تصویر هر کد λ–ثابت‌دوری روی R_s یک کد θ –ثابت‌دوری روی میدان F_{p^m} باشد. در این مقاله به بررسی وجود (λ,θ)–تابع‌های گری روی R_s می‌پردازیم. در این راستا، یک شرط معادل برای چنین توابعی می‌یابیم. سپس ثابت می‌کنیم که اگر Φ یک (λ,θ)–تابع گری به‌طول l روی R_s باشد و $\lambda=\lambda_0+\lambda_1u+\cdots+\lambda_{s-1}u^{s-1}$ 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 به‌طول 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 به‌طول n روی حلقهٔ R، یک زیرمجموعه از R^n است. کد C را یک کد خطی گوییم هرگاه یک R–زیرمدول R^n باشد. به حلقهٔ R الفبای کد گوییم. کد C را α–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[1] و در حالتی که داشته باشیم $\alpha=-1$، کد را منفی‌دوری[2] 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[3] 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. ولفمن [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[4] روی حلقه‌ها و کدهای ثابت‌دوری روی میدان‌ها را فراهم آورد. در ادامه، با ارائه 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] به‌دست 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 حلقهٔ موردنظر را به دستهٔ خاصی از کدها روی میدان متناهی، داراست. مثلا 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 حلقهٔ $R_s = \frac{F_{p^m}[u]}{\langle u^s \rangle}$ و تعریف یک $(\lambda, \theta)-$تابع گری، به‌عنوان 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 Φ یک $(\lambda, \theta)-$تابع گری به‌طول l روی R_s باشد و $\lambda = \lambda_0 + \lambda_1 u + \cdots + \lambda_{s-1} u^{s-1}$ آن‌گاه داریم $\theta = \lambda_0^{\,l}$ و p، طول Φ یعنی l را می‌شمارد. هم‌چنین ثابت می‌کنیم که 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 روی R_s معرفی می‌کنیم که در آن λ عضو وارون‌پذیر دل‌خواهی از R_s است.

برخی پیش‌نیازها: کدهای ثابت‌دوری و حلقهٔ R_s

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

تعریف ۱. فرض کنید R یک حلقهٔ متناهی دل‌خواه باشد. یک کد C به‌طول n روی R، یک زیرمجوعهٔ R^n است. کد C را خطی گوییم هرگاه $R-$زیرمدول R^n باشد.

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

تعریف ۳. فرض کنید p یک عدد اول و m, s دو عدد طبیعی باشند. هم‌چنین فرض کنید F_{p^m} میدان متناهی از مرتبهٔ p^m است و $F_{p^m}[u]$ نمایان‌گر حلقهٔ چندجمله‌ای‌ها روی F_{p^m} با متغیر u باشد. حلقهٔ R_s را برابر حلقهٔ خارج‌قسمتی

$$\mathrm{R}_s := \frac{F_{p^m}[u]}{\langle u^s \rangle}$$

تعریف می‌کنیم.

مشخص است که حلقهٔ R_s یک حلقهٔ جابه‌جایی و یکدار متناهی از اندازهٔ p^{ms} است. از طرفی، بنابر قضیهٔ XVII.5 از [۷]، R_s یک حلقهٔ زنجیری و لذا یک حلقهٔ موضعی با ایده‌ال ماکزیمال $\langle u \rangle$ است. هر عنصر r متعلق به R_s را می‌توان به‌صورت $r = r_0 + r_1 u + \cdots + r_{s-1} u^{s-1}$ نوشت که $r_i \in F_{p^m}$. چون در یک حلقهٔ موضعی، مجموعهٔ 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 (λ,θ)–تابع گری

در این بخش به تعریف تابع گری روی R_s پرداخته و (λ,θ)–تابع گری را نیز تعریف می‌کنیم. در ادامهٔ بخش، شرایط معادلی را برای این که یک تابع Φ، یک (λ,θ)–تابع گری باشد بیان و اثبات می‌کنیم.

تعریف ۴. منظور از یک تابع گری ϕ به‌طول 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 $r=r_0+r_1u+\cdots+r_{s-1}u^{s-1}$، تصویر گری r را برابر با حاصلضرب بردار $[r_0,r_1,\dots,r_{s-1}]$ در ماتریس ϕ 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

$$\begin{aligned}\phi(\mathrm{v})=(&\phi_0(\mathrm{v}_0),\phi_0(\mathrm{v}_1),\dots,\phi_0(\mathrm{v}_{N-1}),\\&\phi_1(\mathrm{v}_0),\phi_1(\mathrm{v}_1),\dots,\phi_1(\mathrm{v}_{N-1}),\\&\phi_{l-1}(\mathrm{v}_0),\phi_{l-1}(\mathrm{v}_1),\dots,\phi_{l-1}(\mathrm{v}_{N-1})).\end{aligned}$$

تعریف ۵. فرض کنید λ عضو وارون‌پذیری از R_s و θ عضو وارون‌پذیری از F_{p^m} باشند. تابع گری ϕ را یک (λ,θ)-تابع گری گوییم هرگاه تصویر هر کد λ–ثابت‌دوری روی R_s به‌وسیلهٔ ϕ، یک کد θ-ثابت دوری روی F_{p^m} باشد.

تعریف ۶. فرض کنید R یک حلقه و λ عضو وارون‌پذیری از R باشد. جایگشت σ_λ روی R^N را به‌صورت

$$\sigma_\lambda(\mathrm{v}_0,\mathrm{v}_1,\dots,\mathrm{v}_{N-1})=(\lambda\mathrm{v}_{N-1},\mathrm{v}_0,\dots,\mathrm{v}_{N-2})$$

تعریف می‌کنیم.

قضیهٔ ۷. شرایط زیر معادل‌اند:

الف) ϕ یک (λ,θ)-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 $\phi\left(\sigma_\lambda(v)\right)=\sigma_\theta(\phi(v))$.

اثبات: از ب) به ج) و از ج) به الف) بدیهی است. تنها الف) به ب) را اثبات می‌کنیم. فرض کنید ϕ یک (λ,θ)-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 δ در R_s موجود است که $\delta^N=\lambda$. حال قرار دهید

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

یعنی C همان R_s-زیرمدول دوری تولید شده به‌وسیلهٔ $\left(\delta^{N-1},\delta^{N-2},\dots,\delta,1\right)$ از R_s-مدول ${R_s}^N$ است. می‌توان دید که C یک کد λ-ثابت‌دوری است. چون ϕ یک (λ,θ)-تابع گری است باید برای یک $b\in R_s$ داشته باشیم

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

به‌عبارت دیگر باید داشته باشیم

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

$$\phi_{l-2}(a), \phi_{l-1}\left(a\delta^{N-1}\right), \dots, \phi_{l-1}(a\delta)) \quad .$$

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

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

با توجه به دل‌خواه بودن a، حکم ثابت است.

اکنون فرض کنید $r = r_0 + r_1 u + \cdots + r_{s-1}u^{s-1}$ عضوی از R_s باشد و قرار دهید

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

به‌علاوه قرار دهید

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

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

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

حال شرط دوم از قضیهٔ قبل معادل است با این که

$$M_\lambda \phi = \phi D_\theta. \qquad (۱)$$

فرض کنید

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

اگر بنویسیم $\lambda = \lambda_0 + \lambda_1 u + \cdots + \lambda_{s-1}u^{s-1}$ آن‌گاه معادلهٔ(۱) معادل است با

$$\begin{pmatrix} \lambda_0 & \lambda_1 & \cdots & \lambda_{s-2} & \lambda_{s-1} \\ 0 & \lambda_0 & \cdots & \lambda_{s-3} & \lambda_{s-2} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & \lambda_0 \end{pmatrix} \begin{pmatrix} g_{0,0} & g_{0,1} & & g_{0,l-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,l-1} \\ \vdots & & \ddots & \vdots \\ g_{s-1,0} & g_{s-1,1} & \cdots & g_{s-1,l-1} \end{pmatrix} =$$

$$\begin{pmatrix} \theta g_{0,l-1} & g_{0,0} & & g_{0,l-2} \\ \theta g_{1,l-1} & g_{1,0} & \cdots & g_{1,l-2} \\ \vdots & & \ddots & \vdots \\ \theta g_{s-1,l-1} & g_{s-1,0} & \cdots & g_{s-1,l-2} \end{pmatrix}. \qquad (۲)$$

قضیهٔ ۸. اگر ϕ یک (λ, θ)-تابع گری به‌طول l روی R_s باشد آن‌گاه $\lambda_0^{\,l} = \theta$ و عضو غیر صفر δ در F_{p^m} موجود است که سطر sام ماتریس ϕ 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 sام از ماتریس‌های رابطهٔ (۲) داریم $\lambda_0 g_{s-1,0} = \theta g_{s-1,l-1}$ و هم‌چنین برای هر i که $1 \le i \le s-1$ 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 sام ماتریس ϕ برابر صفر میشود که در تناقض با رتبهٔ کامل بودن ϕ است. پس داریم $\lambda_0^{\,l} = \theta$ و با قرار دادن $g_{s-1,l-1} := \delta$ حکم ثابت است. اکنون اگر $\theta = 1$ آن‌گاه باید داشته باشیم $\lambda_0^{\,l} = 1$ چون λ_0 عضوی از گروه ضربی میدان F_{p^m} است پس باید مرتبه λ_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 $\lambda_0 = 1$.

قضیهٔ ۹. اگر ϕ یک (λ, θ)-تابع گری به‌طول l روی R_s باشد آن‌گاه باید داشته باشیم $\lambda_1 \neq 0$ و $p|l$. هم‌چنین عضو γ در F_{p^m} موجود است که سطر $(s-1)$ام ماتریس ϕ برابر است با

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

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

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

و برای $0 \le i \le l-2$ 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 sام ماتریس ϕ 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 $0 \le i \le l-2$ 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 λ_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 λ_0 و δ غیرصفر هستند. اگر $\lambda_1 = 0$ و هم‌چنین $g_{s-2,l-1} = 0$ آن‌گاه سطر $(s-1)$ام ماتریس ϕ برابر صفر می‌شود و اگر $\lambda_1 = 0$ و $g_{s-2,l-1}$ عضو غیرصفری مانند γ باشد آن‌گاه سطر $(s-1)$ام ماتریس ϕ برابر مضربی از سطر sام آن می‌شود که در هر دو صورت با رتبهٔ کامل بودن ϕ در تناقض است. از این رو داریم $\lambda_1 \neq 0$ و هم‌چنین $g_{s-2,l-1}$ عضو غیرصفری مانند γ است. حال می‌توان از $-l\lambda_1\lambda_0^{\,l-1}\delta = 0$ نتیجه گرفت که $l = 0$ و این یعنی مشخصهٔ میدان یا همان p، طول تابع گری یا همان l را می‌شمارد. به‌علاوه سطر $(s-1)$ام ماتریس ϕ نیز چنان‌که ادعا شده بود، به‌دست می‌آید.

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

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

نتیجهٔ ۱۰. اگر λ از نوع t باشد که $t \geq 2$، آن‌گاه هیچ (λ, θ)-تابع گری روی R_s موجود نیست. به‌علاوه همهٔ کدهای به‌دست آمده از تصویر کدهای ثابت‌دوری روی R_s به‌وسیلهٔ یک (λ, θ)-تابع گری، کدهای ثابت‌دوری با ریشهٔ تکراری هستند.

در نتیجهٔ ۱۱، تمام (λ, θ)-توابع گری روی R_2 را رده‌بندی می‌کنیم. اثبات آن از قضیهٔ ۹ نتیجه می‌شود.

نتیجهٔ ۱۱. هر (λ, θ)-تابع گری ϕ با طول $l = pl'$ روی R_2 بدین‌صورت است:

$$\phi = \left[{\lambda_0}^{(l'-1)p} \phi' \,|\, \ldots \,|\, {\lambda_0}^{p} \phi' \,|\, \phi' \right]$$

که در آن

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

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 نتیجهٔ ۱۱، داریم $\lambda_0 = 1$، $\lambda_1 = 2$، $l' = 1$ و $p = 3$. هم‌چنین، δ و γ 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 $\gamma = 1$، $\delta = 2$ و بنابراین

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

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

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

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

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

از این رو ϕ_1، ϕ_2، ϕ_3 و ϕ_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 (λ, θ)-توابع گری را به‌دست آوردیم و هم‌چنین شرایط لازم خوبی را برای وجود این توابع به‌دست آوردیم ولی با چنین تحلیلی، به‌سختی می‌توان یک (λ, θ)-تابع گری برای R_s در حالت کلی ساخت. در واقع دقت کنید که حتی می‌توانیم یک (λ, θ)-تابع گری روی R_s را که $\lambda = \lambda_0 + \lambda_1 u + \cdots + \lambda_{s-1} u^{s-1}$، به یک (λ', θ)-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 نمی توان برای یافتن یک (λ, θ)-تابع گری برای R_s در حالت کلی، به کار برد.

در حالت خاص می توانیم با روش دیگری به حل چنین مسئله‌ای بپردازیم. در بخش بعد، وقتی که $s = p^k$ توانی از عدد اول p است، یک (λ, θ)-تابع گری به‌طول s روی R_s می‌سازیم.

نکته ۱۳. بدیهی است که اگر ϕ یک (λ, θ)-تابع گری به‌طول s روی R_s باشد و هم‌چنین $1 \leq t \leq s$، آن‌گاه ϕ_t که متشکل از t سطر آخر ϕ است، یک $(\bar{\lambda}, \theta)$-تابع گری به‌طول s روی R_t است که در آن

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

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 به‌طول s روی R_s می‌سازیم. ابتدا دقت کنید که اگر

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

آن‌گاه $\lambda_0, \lambda_1 \neq 0$ از این‌رو می‌توانیم بنویسیم $\lambda = \lambda_0 + \alpha u$ که در آن $\alpha = \lambda_1 + \lambda_2 u + \cdots + \lambda_{s-1} u^{s-2}$ عضو وارون‌پذیری از R_s است. بدیهی است که R_s یک فضای برداری با بعد s روی F_{p^m} است که $A = \{1, u, u^2, \ldots, u^{s-1}\}$ 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 مجموعهٔ $B = \left\{1, \lambda, \lambda^2, \ldots, \lambda^{s-1}\right\}$ نیز یک پایه برای فضای برداری R_s روی F_{p^m} است.

اکنون متناظر با پایه‌های A و B یک ماتریس تبدیل پایهٔ $G_{A,B}$ موجود است که اگر $r = r_0 + r_1 u + \cdots + r_{s-1} u^{s-1}$ عضوی از R_s باشد و

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

آن‌گاه داریم $r = a_0 + a_1 \lambda + \cdots + a_{s-1} \lambda^{s-1}$.

قضیهٔ ۱۵. $G_{A,B}$ یک $(\lambda, \lambda_0^{\,s})-$تابع گری به‌طول s روی R_s است.

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

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

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

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

و اثبات تمام است.

اکنون با توجه به نکتهٔ قبل، برای هر t که $p^{k-1} < t \leq p^k$ می‌توان یک تابع گری به‌طول 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 $r = a_0 + a_1 \lambda + \cdots + a_{s-1} \lambda^{s-1}$ آن‌گاه $r = r_0 + r_1 u + \cdots + r_{s-1} u^{s-1}$ که در آن

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

و H_λ ماتریسی است که درایه (i, j) آن برابر $\binom{i}{j} \lambda_0^{\,i-j}$ است. اکنون می‌توان دید که ماتریس G_λ که درایه (i, j) آن برابر $(-1)^{i+j} \binom{i}{j} \lambda_0^{\,i-j}$ است، وارون ماتریس H_λ است و از این رو داریم

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

پس ماتریس $\phi = G_\lambda$ یک $(\lambda, \lambda_0^{\ s})$–تابع گری به‌طول 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., Kummar 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 $F_p+uF_p+\cdots+u^kF_p$", J. Hefei Univ. Technol. Nat. Sci., 29 (2006) 1049-1052.