数 学 年 刊 A 辑
2021, 42(2):149–158
DOI: 10.16205/j.cnki.cama.2021.0012

与对角格空时码相关的一类 $\mathbb{Z}[\zeta_m]$ 上不可约多项式的判别式*

杨仕椿[1] 廖群英[2]

提要 为实现信号在空间的分集, 关于格的空时分组码的设计近年来备受关注. 通过研究与对角的格空时码相关的 $\mathbb{Z}[\zeta_m]$ 上的一类二次不可约多项式的判别式 $|\Delta|$, 确定了 $\mathbb{Z}[\zeta_m]$ 上的格空时编码的正规分集乘积的大小. 进而, 利用 Pell 方程的解的性质, 构造性地证明了 $m=5,8,10,12$ 时, $|\Delta|$ 的值可以任意小. 最后, 提出几个关于 $\mathbb{Z}[\zeta_m]$ 上的二次不可约和三次不可约多项式的判别式大小的猜想.

关键词 判别式, 不可约多项式, Pell 方程, 对角格空时码
MR (2000) 主题分类 11Z05, 06B99, 15A15
中图法分类 O156.1
文献标志码 A
文章编号 1000-8314(2021)02-0149-10

1 引言及主要结论

空时编码 (space-time code) 是一种多天线系统中的信道编码技术, 是目前信息通信研究的一个热点, 能极大提高频谱利用率, 是一种充满希望的新型关键技术[1−9]. 为实现信号在空间的分集, 关于格 (lattice) 的空时分组码的设计近年来备受关注[1,10−13]. 由于格空时码能够达到编译码复杂度、性能和频带利用率之间的最佳折衷, 人们基于数论、代数、组合等的方法和技巧, 构造出很多性能优良的格空时码[14−24].

令 $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$ 分别为全体复数、有理数、整数的集合, 定义 $M_n(\mathbb{C})$ 为 $\mathbb{C}$ 上 $n\times n$ 矩阵的全体. 格空时码是指集合 $M_n(\mathbb{C})$ 的一个 $n\times n$ 矩阵集合 $\mathcal{A}$, 使得 $\mathcal{A}$ 在矩阵的加法运算下是一个自由 Abel 群. 定义格空时码 $\mathcal{A}$ 的秩 (rank) 即为该 Abel 群的秩. $M_n(\mathbb{C})$ 的格空时码 $\mathcal{A}$ 的分集乘积定义为:

$$\xi(\mathcal{A})=\inf\{|\det(A-B)|: A,B\in\mathcal{A}, A\neq B\}.$$

$\mathcal{A}$ 的正规分集乘积 (normalized diversity product)d_g 定义为[12,15,18,21]:

$$d_g=\frac{\xi(\mathcal{A})}{|\det G|\cdot|L|^{\frac{n}{2}}}=\frac{\xi(\mathcal{A})}{\sqrt{|\det g|}}, \tag{1.1}$$

本文 2020 年 4 月 12 日收到, 2020 年 11 月 20 日收到修改稿.
[1]阿坝师范学院数学学院, 四川 汶川 623002. E-mail: ysc1020@sina.com
[2]四川师范大学数学科学学院, 成都 610066. E-mail: qunyingliao@sicnu.edu.cn
*本文受到国家自然科学基金 (No. 11861001, No. 12071321), 四川省应用基础研究项目 (No. 2016JY0134, No. 2018JY0458) 和四川省高校科研创新团队建设计划 (No. 18TD0047) 的资助.

这里 G 为格空时码 $\mathcal{A}$ 相应的生成矩阵, g 是 G 相应的实生成矩阵, $|L|$ 表示二维实基格空时码 L 的 2×2 的生成矩阵的行列式的绝对值. 一个良好的格空时码应具有较大的正规分集乘积 d_g. 文 [10, 16–20] 中给出了一些集合 K 上的具有较大 d_g 的格空时码 $\mathcal{A}$. 但在一个给定的集合上求具有最大的正规分集乘积 d_g 的最优格空时码 $\mathcal{A}$, 仍然是一个公开问题[12,16].

设 $\zeta_m=\exp(\frac{2\pi \mathrm{i}}{m})$. 在构造关于分圆环 $\mathbb{Z}[\zeta_m]$ 上的一类对角格空时编码 $\mathcal{D}$ 时, 文 [12] 研究了 $\mathcal{D}$ 相应的生成矩阵 G 的大小. 根据多项式理论可知, 此时 G 的值满足

$$\Delta=(\det G)^2,$$

其中 Δ 是 $\mathcal{D}$ 的相应的最小多项式 $f(x)$ 的判别式 (见 [12]). 对于 $\mathbb{Z}[\zeta_m]$ 上的二次不可约多项式 $f(x)=x^2+bx+c$, 设 $b=u+v\zeta_m$, $c=s+t\zeta_m$, $u,v,s,t\in\mathbb{Z}$, 则其判别式

$$\begin{aligned}\Delta_m&=b^2-4c=(u+v\zeta_m)^2-4(s+t\zeta_m)\\&=u^2-4s-v^2+2\zeta_m\Big(uv-2t+v^2\cos\frac{2\pi}{m}\Big).\end{aligned}\tag{1.2}$$

文 [12] 证明了: 当 $m=4,6$ 时, 对任意 $b,c\in\mathbb{Z}[\zeta_m]$, 均有

$$|\Delta_4|\geqslant 3,\quad |\Delta_6|\geqslant\sqrt{13},\tag{1.3}$$

而且 (1.3) 中等号均可以取到. 由于在 $\mathbb{Z}[\zeta_4](=\mathbb{Z}[\mathrm{i}])$ 上以及 $\mathbb{Z}[\zeta_6]$ 上, 均有 $\xi(\mathcal{A})=1$(见 [16, 25]), 从而对于这一类对角的格空时编码 $\mathcal{D}$, 分别有 $d_g\leqslant\frac{1}{\sqrt{3}}$ 以及 $d_g\leqslant\frac{1}{\sqrt[4]{13}\frac{\sqrt{3}}{2}}$, 因此, 此时的 $\mathcal{D}$ 具有最优的正规分集乘积.

由 (1.1) 可得知, 给定集合 K 上的不可约多项式的判别式值的大小, 可以决定 K 上格空时编码的正规分集乘积, 由此可以构造出相应的性能优良的格空时编码. 因此, 研究不可约多项式的判别式值的大小有着重要的意义. 本文考虑 $\mathbb{Z}[\zeta_m]$ 上的二次不可约多项式 $f(x)=x^2+bx+c$ 的判别式. 由于 $\mathbb{Z}[\zeta_3]=\mathbb{Z}[\zeta_6]$, 因此我们只考虑 $m\neq 3,4,6$ 的情形. 对于 $m=5,8,10,12$, 利用 Pell 方程的解的性质, 我们得到与 (1.3) 相反的结论, 构造性地证明了 $|\Delta_m|$ 可以任意小. 事实上, 我们证明了如下定理.

定理 1.1 当 $m=5,8,10,12$ 时, 对任意给定的正实数 ε, 均存在 $\mathbb{Z}[\zeta_m]$ 上的二次不可约多项式

$$f(x)=x^2+bx+c,$$

使得 $0<|\Delta_m|<\varepsilon$.

对于其他的 m 值, 我们猜想: $|\Delta_m|$ 的值可以任意小. 在本文末, 我们给出一些 $|\Delta_m|$ 比较小的例子, 提出一些有待于进一步研究的问题.

2 引　理

引理 2.1 设 p 为素数, k 为正整数, $v_p(n)$ 满足 $p^{v_p(n)}\,|\,n$ 且 $p^{v_p(n)+1}\nmid n$, 则

$$v_p\Big(\binom{p^k}{j}\Big)\geqslant k-v_p(j),\quad 1\leqslant j\leqslant p^k-1. \tag{2.1}$$

证 由

$$\binom{p^k}{j}=\frac{p^k(p^k-1)\cdots(p^k-l+1)}{j(j-1)!}$$

以及 $(j-1)!\,|\,(p^k-1)\cdots(p^k-j+1)$, 知 (2.1) 成立.

引理 2.2 设 $f(x)=x^2+bx+c=x^2+(u+v\zeta_m)x+(s+t\zeta_m)$ 在 $\mathbb{Z}[\zeta_m]$ 上可约, 且 1, ζ_m 和 ζ_m^2 在 $\mathbb{Z}$ 上线性无关, 则存在 $p,q,w\in\mathbb{Z}$, 使得

$$u=p+q,\quad v=w,\quad s=pw,\quad t=qw. \tag{2.2}$$

证 由于 $f(x)=x^2+bx+c$ 在 $\mathbb{Z}[\zeta_m]$ 上可约, 不妨设

$$f(x)=(x+(p+q\zeta_m))(x+(w+l\zeta_m)),$$

其中 $p,q,w,l\in\mathbb{Z}$. 于是

$$\begin{aligned}b&=u+v\zeta_m=p+q+(w+l)\zeta_m,\\ c&=s+t\zeta_m=pw+(pl+qw)\zeta_m+ql\zeta_m^2.\end{aligned} \tag{2.3}$$

由于 1, ζ_m 和 ζ_m^2 在 $\mathbb{Z}$ 上线性无关, 因此 $ql=0$. 不妨设 $l=0$, 由 (2.3) 即可得 (2.2).

3　定理的证明

当 $m=5$ 时, 由 (1.2) 可得

$$\Delta_5=u^2-4s-v^2+2\Big(\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}\Big)\Big(uv-2t+v^2\cos\frac{2\pi}{5}\Big). \tag{3.1}$$

考虑 Pell 方程

$$x^2-5y^2=1,\quad x,y\in\mathbb{N}. \tag{3.2}$$

由于方程 (3.2) 的最小正整数解为 $x_1=9,\ y_1=4$, 则方程 (3.2) 的所有正整数解 (x_n,y_n) 可表为

$$x_n+y_n\sqrt{5}=(9+4\sqrt{5})^n,\quad n\in\mathbb{N}, \tag{3.3}$$

而且

$$0<x_n-y_n\sqrt{5}=\frac{1}{x_n+y_n\sqrt{5}}<\frac{1}{2\sqrt{5}y_n}. \tag{3.4}$$

令 $y_n = 2^{l_n} y'_n$, 其中 y'_n 为奇数. 取 $n = 2^k$, $k \geqslant 2$, $k \in \mathbb{N}$, 由 (3.3) 可得

$$y_n = \binom{n}{1} 9^{n-1} \cdot (4\sqrt{5}) + \cdots + \binom{n}{j} 9^{n-j} \cdot (4\sqrt{5})^j + \cdots + \binom{n}{n-1} 9 \cdot (4\sqrt{5})^{n-1}. \tag{3.5}$$

当奇数 j 满足 $3 \leqslant j \leqslant n-1$ 时, 利用引理 2.1 可得

$$v_2\Big(\binom{n}{j} 9^{n-j} \cdot (4\sqrt{5})^j\Big) \geqslant k - v_2(j) + 2j = k + 2j \geqslant k + 6.$$

特别地, 当 $j = 1$ 时, 有 $v_2\Big(\binom{n}{n-1} 9^{n-1} \cdot (4\sqrt{5})\Big) = v_2(4n) = k + 2$, 故

$$v_2(y_n) = v_2(y_{2^k}) = k + 2. \tag{3.6}$$

于是 $l_{2^k} = k + 2$. 取

$$v^2 = 16 y_n y'_n = 2^{k+6} y'^2_n, \quad 4uv - 8t - v^2 = -16 x_n y'_n, \quad u^2 - 4s - v^2 = 0, \quad 2 \,|\, k, \tag{3.7}$$

注意到 $\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$, 则由 (3.1), (3.4) 以及 (3.7) 可得

$$\begin{aligned} 0 < |\Delta_5| &= \Big|2\zeta_5 \Big(uv - 2t + v^2 \cos \frac{2\pi}{5}\Big)\Big| = \frac{1}{2} |4uv - 8t - v^2 + \sqrt{5} v^2| \\ &= 8(x_n y'_n - y_n y'_n \sqrt{5}) < \frac{4 y'_n}{\sqrt{5} y_n} = \frac{4}{\sqrt{5} \cdot 2^{k+2}} < \frac{1}{2^{k+1}}. \end{aligned} \tag{3.8}$$

我们断言方程 (3.7) 必有整数解 u, v, s, t. 事实上, 由 (3.7) 可知 $v = 2^{\frac{k}{2}+3} \cdot y'_n$. 设 $u = 2u_1$, $u_1 \in \mathbb{Z}$, 且 $\gcd(u_1, y'_n) = 1$, 则由 (3.7) 可得

$$\begin{aligned} t &= \frac{1}{8} v^2 - \frac{1}{2} uv - 2 x_n y'_n = 2 y_n y'_n - u_1 2^{\frac{k}{2}+3} \cdot y'_n - 2 x_n y'_n, \\ s &= \frac{1}{4}(u^2 - v^2) = u_1^2 - 4 y_n y'_n. \end{aligned} \tag{3.9}$$

因此方程 (3.7) 有整数解 u, v, s, t. 同时, 若多项式 $f(x) = x^2 + bx + c$ 可约, 则由引理 2.2 可知, 存在 $p, q, w \in \mathbb{Z}$, 使得

$$u = 2u_1 = p + q, \quad v = 2^{\frac{k}{2}+3} y'_n = w, \quad s = pw, \quad t = qw.$$

于是 $y'_n \,|\, t$, 从而 $y'_n \,|\, u$, 此与 u_1 的取法矛盾.

所以, 可以取偶数 $k > \lfloor \frac{-\log \varepsilon}{\log 2} \rfloor - 1$, 这里 $\lfloor x \rfloor$ 表示不超过实数 x 的最大整数, 从而由 (3.8) 可得

$$0 < |\Delta_5| < \frac{1}{2^{k+1}} < \varepsilon.$$

当 $m = 10$ 时, 由于 $\cos \frac{2\pi}{10} = \frac{\sqrt{5}+1}{4}$, 类似可知对任意正实数 ε, 均存在 $b, c \in \mathbb{Z}[\zeta_{10}]$, 使得

$$0 < |\Delta_{10}| < \varepsilon.$$

当 $m = 8$ 时, 由于 $\zeta_8 = \cos \frac{2\pi}{8} + \mathrm{i} \sin \frac{2\pi}{8} = \frac{\sqrt{2}}{2}(1 + \mathrm{i})$, $\zeta_8^2 = \mathrm{i}$, 则由 (1.2) 式可得

$$\Delta_8 = u^2 - 4s + \sqrt{2}(uv - 2t) + \mathrm{i}(v^2 + \sqrt{2}(uv - 2t)). \tag{3.10}$$

考虑 Pell 方程

$$x^2-2y^2=1,\quad x,y\in\mathbb{N}.$$

由于该方程的最小正整数解为 $x_1=3,y_1=2$, 故方程的全部正整数解 (x_n,y_n) 可表为

$$x_n+y_n\sqrt{2}=(3+2\sqrt{2})^n,\quad n\in\mathbb{N},\tag{3.11}$$

且

$$0<x_n-y_n\sqrt{2}=\frac{1}{x_n+y_n\sqrt{2}}<\frac{1}{x_n}.\tag{3.12}$$

令 $x_n=3^{l_n}x_n'$, 其中 $\gcd(3,x_n')=1$. 取 $n=3^k$, $k\geqslant 2$, $k\in\mathbb{N}$, 则由 (3.11) 可得

$$\begin{aligned}x_n=3^n+\binom{n}{2}3^{n-2}\cdot(2\sqrt{2})^2+\cdots+\binom{n}{j}3^{n-j}\cdot(2\sqrt{2})^j\\+\cdots+\binom{n}{n-1}3\cdot(2\sqrt{2})^{n-1}.\end{aligned}\tag{3.13}$$

当 $j\leqslant n-3$ 为偶数时, 设 $j=3^rj_0$, $\gcd(3,j_0)=1$, $0\leqslant r\leqslant k-1$. 若 $r\geqslant 1$, 则由引理 2.1 知

$$\begin{aligned}v_3\Big(\binom{n}{j}3^{n-j}\cdot(2\sqrt{2})^j\Big)&\geqslant k-v_3(j)+n-j=k-r+3^k-3^rj_0\\&=k-r+3^r(3^{k-r}-j_0)\geqslant k-r+3^r\geqslant k+2.\end{aligned}\tag{3.14}$$

若 $r=0$ 时, 则由 $j\leqslant n-3$ 知 (3.13) 也成立, 且 $v_3\Big(\binom{n}{n-1}3\cdot(2\sqrt{2})^{n-1}\Big)=v_3(3n)=k+1$, 故

$$v_3(x_n)=v_3(x_{3^k})=k+1,\tag{3.15}$$

于是 $l_{3^k}=k+1$. 现在取 $v=2\cdot 3^{\frac{k+1}{2}}x_n'$, $u=2u_1$, $k,u_1\in\mathbb{Z}$, 其中 k 为奇数, $\gcd(u_1,3\cdot x_n')=1$, 且

$$t=2\cdot 3^{\frac{k+1}{2}}x_n'u_1-2y_nx_n',\quad s=\frac{1}{4}(u^2-v^2)=u_1^2-3^{k+1}x_n'^2,$$

则有

$$uv-2t=4y_nx_n',\quad u^2-4s=v^2=4\cdot 3^{k+1}x_n'^2.\tag{3.16}$$

故由 (3.12) 可得

$$0<v^2-(uv-2t)\sqrt{2}=4x_nx_n'-4y_nx_n'\sqrt{2}<\frac{4x_n'}{x_n}=\frac{4}{3^{k+1}}.\tag{3.17}$$

而且类似地, 由引理 2.2 同理可证, 此时多项式 $f(x)=x^2+bx+c$ 在 $\mathbb{Z}[\zeta_8]$ 上是不可约的.

因此, 可取奇数 $k>\lfloor\frac{\log 4\sqrt{2}-\log\varepsilon}{\log 3}\rfloor$, 从而由 (3.10), (3.16)–(3.17) 可得

$$0<|\Delta_8|=(v^2-(uv-2t)\sqrt{2})\sqrt{2}<\frac{4\sqrt{2}}{3^{k+1}}<\varepsilon.$$

当 $m=12$ 时, 由 (1.2) 可得

$$\Delta_{12}=u^2-4s-v^2+\Big(\frac{\sqrt{3}}{2}+\frac{1}{2}\mathrm{i}\Big)(2uv-4t-\sqrt{3}v^2).\tag{3.18}$$

考虑 Pell 方程 $x^2-3y^2=1$, 它的所有正整数解 (x_n,y_n) 可表为 $x_n+y_n\sqrt{3}=(2+\sqrt{3})^n$, $n\in\mathbb{N}$. 令 $n=2^k$, 由引理 2.1 类似地可得

$$v_2(y_n)=v_2(y_{2^k})=k+1. \tag{3.19}$$

利用上面的方法同理可证: 对任意正实数 ε, 均存在 $b,c\in\mathbb{Z}[\zeta_{12}]$, 使得 $0<|\Delta_{12}|<\varepsilon$.

于是, 定理得证.

4 注 记

当 $m=7,9,11,13$ 时, 我们通过 Maple 软件计算给出以下四个例子, 这些 $\mathbb{Z}[\zeta_m]$ 上的不可约多项式的判别式的绝对值都很小.

例 4.1 $\mathbb{Z}[\zeta_7]$ 上的不可约多项式 $f_1(x)=x^2-(282987-282989\zeta_7)x-282988-15075707587\zeta_7$, 其判别式为:

$$|\Delta_7|=|4.0853\cdot 10^{-6}+5.1228\cdot 10^{-6}\mathrm{i}|=6.5504\cdot 10^{-6}.$$

例 4.2 $\mathbb{Z}[\zeta_9]$ 上的不可约多项式 $f_2(x)=x^2-(187381-244609\zeta_9)x-6180480930+44664\zeta_9$, 其判别式为:

$$|\Delta_9|=|5.1693\cdot 10^{-8}+4.3376\cdot 10^{-8}\mathrm{i}|=6.7480\cdot 10^{-8}.$$

例 4.3 $\mathbb{Z}[\zeta_{11}]$ 上的不可约多项式 $f_3(x)=x^2-(102286-102290\zeta_{11})x-204576-830296938\zeta_{11}$, 其判别式为:

$$|\Delta_{11}|=|2.1302\cdot 10^{-5}+1.3690\cdot 10^{-5}\mathrm{i}|=2.5322\cdot 10^{-5}.$$

例 4.4 $\mathbb{Z}[\zeta_{13}]$ 上的不可约多项式 $f_4(x)=x^2-(28062-28060\zeta_{13})x+28061-45121938\zeta_{13}$, 其判别式为:

$$|\Delta_{13}|=|6.5439\cdot 10^{-6}+3.4345\cdot 10^{-6}\mathrm{i}|=7.3904\cdot 10^{-6}.$$

因此, 我们提出如下的猜想.

猜想 4.1 若 $m\neq 3,4,6$, 则对任意正实数 ε, 均存在 $\mathbb{Z}[\zeta_m]$ 上的二次不可约多项式 $f(x)=x^2+bx+c$, 使得

$$0<|\Delta_m|<\varepsilon.$$

对于 $\mathbb{Z}[\zeta_m]$ 上的三次不可约多项式 $f(x)=x^3+bx^2+cx+d$, 当 $m=4,6$ 时, 我们发现其判别式 $|\Delta|$ 都较大, 但如下两个例子中的 $|\Delta|$ 的值较小.

例 4.5 对于 $\mathbb{Z}[\zeta_4]=\mathbb{Z}[\mathrm{i}]$ 上的不可约多项式 $f_5(x)=x^3+x^2+(1-\mathrm{i})x+1$, 其判别式为:

$$|\Delta|=|5+12\,\mathrm{i}|=13.$$

例 4.6[10] 对 $\mathbb{Z}[\zeta_6]$ 上的不可约多项式 $f_6(x)=x^3+(1-\zeta_6)x^2+(1-2\zeta_6)x-\zeta_6$, 其判别式为:

$$|\Delta|=|-13+\sqrt{192}\,\mathrm{i}|=19.$$

由于没有发现 $|\Delta|$ 分别小于 $13,19$ 的例子, 因此我们有下列两个猜想.

猜想 4.2 对于 $\mathbb{Z}[\mathrm{i}]$ 上的三次不可约多项式 $f(x)=x^3+bx^2+cx+d$, 有 $|\Delta|\geqslant 13$.

猜想 4.3 对于 $\mathbb{Z}[\zeta_6]$ 上的三次不可约多项式 $f(x)=x^3+bx^2+cx+d$, 有 $|\Delta|\geqslant 19$.

当 $m\neq 3,4,6$ 时, 通过具体的一些计算我们发现, 这些三次不可约多项式的判别式的值也可以非常小, 因此有如下的猜想.

猜想 4.4 若 $m\neq 3,4,6$, 则对任意给定的正实数 ε, 均存在 $\mathbb{Z}[\zeta_m]$ 上的三次不可约多项式 $f(x)=x^3+bx^2+cx+d$, 使得

$$0<|\Delta|<\varepsilon.$$

参　考　文　献

[1] Bayer-Fluckiger E, Oggier F, Viterbo E. New algebraic constructions of rotated-lattice constellations for the Rayleigh fading channels [J]. *IEEE Trans Inform Theory*, 2004, 50(4):702–714.

[2] Carlos M, Mauro Luiz B, da Silva Eduardo B. New space-time block codes from spectral norm [J]. *PloS ONE*, 2019, 14(9):e0222708.

[3] Garima S, Rashmi G, Raghvendra K, and et al. Space-Time code design using quaternions, octonions and other non-associative structures [J]. *International Journal of Electrical and Computer Engineering Systems*, 2019, 10(2):91–95.

[4] Damen M O, Tewfik A, Belflore J C. A construction of a space-time code based on number theory [J]. *IEEE Trans Inform Theory*, 2002, 48(3):753–760.

[5] Jung H K. Sign reversal channel switching method in space-time block code for OFDM systems, IEICE transactions on fundamentals of electronics [J]. *Communications and Computer Sciences*, 2020, 103(2):567–570.

[6] Mavares T D, Oropeza M, Velásquez R. Space-Time code selection via particle swarm optimization [J]. *Annals of Telecommunications*, 2020, 75(1):59–66.

[7] Srinath K P, Rajan B S. Improved perfect space-time block codes [J]. *IEEE Trans Inform Theory*, 2013, 59(12):7927–7935.

[8] Xu L L, Deng Y Y, Wang Y Q. Application of single carrier STBC in HF communication [J]. *Communication Technology*, 2019, 52(10):2336–2340.

[9] 赵亚军, 郁光辉, 徐汉青. 6G 移动通讯网络: 远景, 挑战与关键技术 [J]. 中国科学: 信息科学, 2019, 49(8):963–987.

[10] Guo X, Xia X G. An elementary condition for non-norm Elements [J]. *IEEE Trans Inform Theory*, 2009, 55(3):1080–1085.

[11] Li Y, Wang H, Xia X G. On quasi-orthogonal space-time block codes for dual-polarized MIMO channels [J]. *IEEE Transactions on Wireless Communications*, 2012, 11(1):397–407.

[12] Liao H, Wang H, Xia X G. Some designs and normalized diversity product upper bounds for lattice-based diagonal and full-rate space-time block codes [J]. *IEEE Trans Inform Theory*, 2009, 55(2):569–583.

[13] Liu W, Lei J, Imran M A, and et al. Diversity gain of lattice constellation-based joint orthogonal space-time block coding [J]. *IET Communications*, 2015, 9(18):2274–2280.

[14] Kundu S, Pados D A, Su W F. Toward a preferred 4×4 space-time block code: a performance-versus-complexity sweet spot with linear-filter decoding [J]. *IEEE Trans Inform Theory*, 2013, 61(5):1847–1855.

[15] Oggier F, Sethuraman B A. Quotients of orders in cyclic algebras and space-time codes [J]. *Advances in Mathematics of Communications*, 2013, 7(4):441–461.

[16] Wang G, Liao H, Wang H, and et al. Systematic and optimal cyclotomic lattices and diagonal space-time block code designs [J]. *IEEE Trans Inform Theory*, 2004, 50(12):3348–3360.

[17] Wang H, Wang G, Xia X G. Some 2×2 unitary space-time codes from sphere packing theory with optimal diversity product of code size 6 [J]. *IEEE Trans Inform Theory*, 2004, 50(12):3361–3368.

[18] Wang G, Xia X G. On optimal multilayer space-time code designs [J]. *IEEE Trans Inform Theory*, 2005, 51(3):1102–1135.

[19] Wang G, Xia X G. Correction to the definition of diversity product in on optimal multi-layer cyclotomic space-time code designs [J]. *IEEE Trans Inform Theory*, 2005, 51(7):2732–2733.

[20] Wang H, Xia X G. Optimal normalized diversity product of 2×2 lattice based diagonal space-time codes from QAM signal constellations [J]. *IEEE Trans Inform Theory*, 2008, 54(12):1814–1818.

[21] Wang H, Zhao Z J. A MIMO system with finite-bit feedback based on fixed constellations [J]. *Science China Information Sciences*, 2013, 56(6):1–14.

[22] Xing C P. Diagonal lattice space-time codes from number fields and asymptotic bounds [J]. *IEEE Trans Inform Theory*, 2007, 53(11):3921–3926.

[23] Xing C P, Li W. A 2×2 lattice space-time code of rank 5 [J]. *Proc Amer Math Soc*, 2008, 136(10):3415–3418.

[24] Yang S C, He B, Togbe A. A 2×2 lattice space-time code of the highest rank [J]. *Proc Amer Math Soc*, 2009, 137(11):3601–3607.

[25] Lang S. Algebraic number fields [M]. New York: Springer-Verlag, 1986.

The Determinant of a Class of Irreducible Polynomials over $\mathbb{Z}[\zeta_m]$ Related to Lattice-Based Diagonal Space-Time Block Codes

YANG Shichun[1]　LIAO Qunying[2]

[1]School of Mathematics, Aba Teachers University, Wenchuan 623002, Sichuan, China. E-mail: ysc1020@sina.com

[2]School of Mathematical Sciences, Sichuan Normal University, Chengdu 610066, China. E-mail: qunyingliao@sicnu.edu.cn

Abstract　To achieve the diversity of the signal in space, the design of the case of space-time block codes has attracted much attention in recent years. By studying the discriminant of a class of quadratic irreducible polynomials over $\mathbb{Z}[\zeta_m]$ related to lattice-based diagonal space-time block codes, the authors determine the size of the normalized diversity product for constructing the lattice space time code over $\mathbb{Z}[\zeta_m]$. Furthermore, based on the property for solutions of the Pell equation, it is proved that the absolute value of the discriminant can be arbitrarily small when $m = 5, 8, 10, 12$. And then for the quadratic or cubic irreducible polynomials over $\mathbb{Z}[\zeta_m]$, some problems to be further studied are proposed.

Keywords Determinant, Irreducible polynomial, Pell equation, Lattice-Based diagonal space-time block code

2000 MR Subject Classification 11Z05, 06B99, 15A15

The English translation of this paper will be published in

Chinese Journal of Contemporary Mathematics, Vol. 42 No. 2, 2021

by ALLERTON PRESS, INC., USA