第17卷第4期 数学研究与评论 Vol. 17 No. 4
1997年11月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Nov. 1997

循环矩阵本原指数的上界估计*

金 晨 辉
(解放军电子技术学院, 郑州450004)

摘 要 本文给出了循环矩阵本原指数上界的新的估计及一种由级数较低的循环矩阵的本原指数估计级数较高的循环矩阵的本原指数的方法, 解决了一类循环矩阵本原指数的计算问题

关键词 循环矩阵, 本原指数
分类号 AMS(1991) 15A30/CCL O151.21

循环矩阵是经常遇到的一类矩阵, 在许多应用问题中占据重要地位. 文献1和文献2解决了循环矩阵的不可约判定和本原性判定问题, 文献3证明了 n 级本原循环矩阵 $E+H^{i_1}+\cdots+H^{i_m}$ 的本原指数不大于 $n/\gcd(i_t,n)+\gcd(i_t,n)-2$, 从而证明了各行至少有三个非零元的 n 级本原循环矩阵的本原指数 $\leq n/2$. 本文将从新的途径研究本原循环矩阵本原指数的上界估计问题, 并对上述结果进行改进.

本文中 $[x]$ 恒表示实数 x 的整数部分, $x\bmod n$ 表示整数 x 被 n 除后所得的余数, $Z/(n)=\{0,1,\cdots,n-1\}$, $\gcd(k,n)$ 表示自然数 k 和 n 的最大公约数, $r(A)$ 表示本原矩阵 A 的本原指数.

本文用 $A=H^{i_1}+\cdots H^{i_m}$ 表示 n 级循环矩阵, 用 E 表示单位矩阵, 其中 $H=(h_{ij})$ 是取值0, 1的矩阵且 $h_{ij}=1$ 当且仅当 $j\bmod n=(i+1)\bmod n$. 一般地, 矩阵 H 的级数由上下文即可看出.

引理1[1,2] n 级循环矩阵 $A=H^{i_1}+\cdots+H^{i_m}$ 是本原矩阵当且仅当 $n, (i_2-i_1)\bmod n,\cdots,(i_m-i_1)\bmod n$ 互素.

引理2[3] 设 n 级循环矩阵 $A=H^{i_1}+\cdots+H^{i_m}$ 是 n 级本原循环矩阵且 $i_1,\cdots,i_m$ 模 n 至少有三个不同元, 则有 $r(A)<n/2$.

引理3 设 $A=E+H^{i_1}+\cdots+H^{i_m}$ 是 n 级本原循环矩阵, 则 $r(A)\leq\alpha$ 当且仅当 $\{(\sum_{i=1}^{m}t_ia_i)\bmod n:\ \sum_{i=1}^{m}t_i\leq\alpha$ 且诸 $t_i\geq 0\}\supset Z/(n)$.

证明 利用 $E+H+H^2+\cdots+H^{n-1}$ 是全1矩阵即可直接验证.

推论1 设 $A=E+H^{a_1}+\cdots+H^{a_m}$, $B=H^c+H^{ba_1+c}+\cdots+H^{ba_m+c}$ 均是 n 级循环矩阵且 $\gcd(b,n)=1$, 则 A 是本原矩阵当且仅当 B 是本原矩阵且有 $r(A)=r(B)$.

推论2 设 $A=E+H+H^{a_1}+\cdots+H^{a_m}$, $B=E+H+H^{n-a_1+1}+\cdots+H^{n-a_m+1}$ 均是 n 级循环矩阵, 则 A 是本原矩阵当且仅当 B 是本原矩阵且 $r(A)=r(B)$.

* 1994年10月18日收到. 1997年3月17日收到修改稿

证明 在推论1中取 $b=c=n-1$ 即证

定理1 设 $A=E+H^{a_1}+\cdots+H^{a_m}$ 为 n 级本原循环矩阵, 又设 $a_1^{-1}a_1 \bmod n=1$, $b=a_1^{-1}a_m \bmod n$, 则有

$$r(A)\leq \min\{[n/b]+b-2,\ [n/(n-b+1)]+n-b-1\}.$$

证明 设 $p=[n/b]$, $x\in Z/(n)$. 如果 $pb\leq x\leq n-1$, 则 $0\leq t=x-pb<b-1$, 故 $x=pb+t$ 且 $p+t\leq p+b-2$; 如果 $0\leq x<pb$, 记 $x=tb+a$ 且 $0\leq a<b$, 则有 $0\leq t<p$, 从而 $a+t\leq b+p-2$, 这表明

$$Z/(n)\subset\{(tb+a)\bmod n:\ t,a\geq 0\text{且}\ t+a\leq b+p-2\},$$

故由引理3知 $r(E+H+H^b)\leq b+p-2$. 同理可证 $r(E+H+H^{n-b+1})\leq[n/(n-b+1)]+n-b-1$, 但 $r(E+H+H^b)=r(E+H+H^{n-b+1})$, 从而

$$r(A)\leq r(E+H+H^b)\leq \min\{[n/b]+b-2,\ [n/(n-b+1)]+n-b-1\}.$$

定理2 设 $A=E+H+H^k$ $(2\leq k<n)$ 为 n 级循环矩阵, k 整除 n, 则 $r(A)=n/k+k-2$

证明 设 $p=n/k$, $\Omega_n=\{(tk+a)\bmod n:\ a,t\geq 0\text{且}\ a+t\leq m\}$. 再设 $x\in\Omega_n$, 则存在非负整数 a, t 和整数 c, 使 $a+t\leq m$ 且 $x=tk+a+cn$. 记 $a=sk+a'$, 其中 $0\leq a'<k$. 令 $T=(s+t)\bmod p$, 则 $x=x\bmod n=Tk+a'$. 显然 $x=n-1$ 当且仅当 $T=p-1$ 且 $a'=k-1$, 此时必有 $m\geq a+t\geq T+a'=p+k-2$, 即 $m<p+k-2$ 时 $Z/(n)\neq\Omega_n$, 故由引理3知 $r(A)\geq p+k-2$, 再由定理1知 $r(A)\leq p+k-2$, 从而 $r(A)=n/k+k-2$

推论 设 $A=E+H+H^k$ $(2\leq k<n)$ 为 n 级循环矩阵, 且 $n-k+1$ 整除 n, 则有

$$r(A)=n/(n-k+1)+n-k-1.$$

定理3 设 $A=E+H^{a_1}+\cdots+H^{a_m}$ 是 n 级本原循环矩阵, 又设 $\gcd(a_m,n)$ 级循环矩阵 $E+H^{a_1}+\cdots+H^{a_{m-1}}$ 的本原指数为 α, 则有 $r(A)\leq n/\gcd(a_m,n)+\alpha-1$.

证明 设 $b=\gcd(a_m,n)$, $p=n/b$. 又设 $x\in Z/(n)$, 则存在非负整数 t, a, 使 $x=tb+a$ 且 $0\leq a<b$, 则 $0\leq t<p$. 因 A 是 n 级本原循环矩阵, 故由引理1知

$$\gcd(a_1,\cdots,a_{m-1},b)=\gcd(a_1,\cdots,a_m,n)=1,$$

故由引理1知 b 级循环矩阵 $E+H^{a_1}+\cdots+H^{a_{m-1}}$ 是本原矩阵, 再由题设知其本原指数为 α, 故由引理3知存在非负整数 $t_1,\cdots,t_{m-1}$ 和整数 d, 使 $t_1+\cdots+t_{m-1}\leq\alpha$, 且有 $a=t_1a_1+\cdots+t_{m-1}a_{m-1}+db$, 故

$$x=(d+t)b+t_1a_1+\cdots+t_{m-1}a_{m-1},$$

因 $b=\gcd(a_m,n)$, 故存在非负整数 $e<p$, 使 $ea_m \bmod n=(d+t)b \bmod n$, 从而有

$$x=(t_1a_1+\cdots+t_{n-1}a_{m-1}+ea_m)\bmod n$$

且 $t_1+\cdots+t_m+e\leq\alpha+p-1$, 这表明

$$Z/(n)\subset\{(\sum_{i=1}^{m}t_ia_i)\bmod n:\ \text{诸}\ t_i\geq 0\ \text{且}\ \sum_{i=1}^{m}t_i\leq\alpha+p-1\},$$

故由引理3知 $r(A)\leq\alpha+p-1=n/\gcd(a_m,n)+\alpha-1$.

推论 设 $A=E+H^{a_1}+\cdots+H^{a_m}$ 为 n 级本原循环矩阵, 如果 $0,a_1,\cdots,a_{m-1}$ 模 $\gcd(a_m,n)$ 至少有三个不同元, 则 $r(A)\leq n/\gcd(a_m,n)+[\gcd(a_m,n)/2]-1$.

证明 由引理2知 $\gcd(a_m,n)$ 级本原循环矩阵 $E+H^{a_1}+\cdots+H^{a_{m-1}}$ 的本原指数 $\leq\gcd(a_m,n)/2$, 再由定理3即证本推论

例 设 $n=2k$, 则 n 级循环矩阵 $A=E+H+H^{k}+H^{n-1}$ 的本原指数 $\leq[n/4]+1$.

证明 不妨设 $k>2$, 则 $0, 1, n-1$ 模 k 互不相同, 且 $\gcd(k, n)=k$, 故由定理3推论知

$$r(A)\leq n/\gcd(k, n)+[\gcd(k, n)/2]-1=[n/4]+1.$$

参 考 文 献

[1] K. H. Kim-Butler and J. R. Krabill, *Circulant boolean relation matrices*, Czechoslovak Math. J., 24 (1974), 247-251.

[2] Š. Schwarz, *Circulant Boolean relation matrices*, Czechoslovak Math. J., 24(1974), 252-253.

[3] Huang Daode, *On circulant Boolean matrices*, Linear Algebra and Its Applications, 136(1990), 107-117.

Estimates for the Upper Bounds of Primitive Exponent of Circulant Matrices

Jin Chenhui

(PLA Electronic Technical College, Zhengzhou 450004)

Abstract

In this paper, we give estimates for the upper bounds of primitive exponent of circulant matrices, give an approach to estimate the primitive exponent of a circulant matrix using the primitive exponent of a related circulant matrix with lower order, and compute the primitive exponents of a class of circulant matrices.

Keywords circulant matrix, primitive exponent.