关于循环群的最小图

周尚超

数学教研室

摘　要

设$\beta(n)$是自同构群是n阶循环群且顶点最少的图的最小边数，当n不被2，3，5整除时，本文得到了$\beta(n)$的数值。本文还构造了自同构群是4阶循环群且顶点最少的12个图，其中边数最小的是18条边。

一、循环群的图的最小边数

§1引　言

设$\alpha(n)$是自同构群是n阶循环群且顶点最少的图的顶点个数，$\beta(F,m)$是群与F同构且有m个顶点的图的最小边数。用$\beta(n)$表示$\beta(C_n,\alpha(n))$，文〔1〕中提出求$\beta(n)$的问题并且得到了$\beta(3)=15$，$\beta(5)=25$。文〔2〕中得到$\beta(C_m,2m)\leqslant 4m$，这里$m=p^e>7$，p是素数。文〔2〕和〔3〕都求过$\alpha(n)$，$\alpha(n)$的数值最后由Meriwether在1963年得到，但其证明未见发表。$\alpha(n)$的数值可由〔4〕或Math Reviews 33(1967) #2563得知。当n不被2，3，5整除时，本文得到了$\beta(n)$的数值。我们对$\beta(n)$的数值的证明蕴含了对$\alpha(n)$的数值的证明。

定理1　设$p\geqslant 7$是素数，则$\beta(p^e)=4p^e$。

定理2　设$n=p_1^{e_1}p_2^{e_2}\cdots\cdots p_r^{e_r}$，$p_i\geqslant 7$是素数，则

$$\beta(n)=4\sum_1^r p_i^{e_i}。$$

§2定理的证明

图G的顶点集用$V=V(G)$表示，边集用$E=E(G)$表示，V上置换σ生成的群用(σ)表

本文第一部分完成于1986年4月第二部分于1985年11月8日收到

中国知网 https://www.cnki.net

示，σ变动的点集用$V(\sigma)$表示。设$\sigma=\sigma_1\sigma_2\cdots\cdots\sigma_k$是$\sigma$不交的轮换分解，$\sigma$的单点轮换略不写，用$|\sigma_i|$表示轮换$\sigma_i$的长度。G的自同构群用Aut G表示，G的以$V_i$为顶点集的导出图用$G_i=G(V_i)$表示，$V_i$的恒等置换用$\varepsilon_i$表示。邻接顶点i，j的边用〔i,j〕表示。$\sigma$〔i,j〕表示边〔$\sigma(i),\sigma(j)$〕。$\sigma(E)$表示边集$\{\sigma$〔i,j〕|〔i,j〕$\in E\}$。

引理1　设$\mathrm{Aut}\,G=(\sigma)$，$\sigma=\sigma_1\sigma_2\cdots\cdots\sigma_k$，$\sigma_1=(1\ 2\cdots\cdots m)$，$m\neq 2$，则一定存在$\sigma_i$ $(i\neq 1)$，使m与$|\sigma_i|$不互素。

证明　设m与任意$|\sigma_i|$ $(i\neq 1)$，互素，设$|\sigma_i|=n$，$V_1=V(\sigma_1)$，$V_i=V(\sigma_i)$，因为$\sigma^n\in \mathrm{Aut}G$，$V_i$中顶点都是$\sigma^n$的不动点，$\sigma^n$在$V_1$上的限制是一个长为m的循环，因此若$d\in V_i$，d与$V_1$中一个顶点邻接，则d与$V_1$中所有顶点邻接。设$\tau_1=(1)(2m)(3\ m-1)\cdots$，则易证$\tau_1\in\mathrm{Aut}G$，矛盾。

系1　设$\mathrm{Aut}G=(\sigma)$，$\sigma^2\neq\varepsilon$，$\sigma=\sigma_1\sigma_2\cdots\cdots\sigma_k$，则$k\geqslant 2$。

系2　设$\mathrm{Aut}G=(\sigma)$是p^e阶群，$p^e\neq 2$，则$|V(G)|\geqslant p^e+p$，这里p是素数。

系3　$\alpha(p^e)\geqslant p^e+p$，$p^e\neq 2$，p是素数。

定理1的证明　设$\sigma=\sigma_1\sigma_2$，$\sigma_1=(1\ 2\cdots\cdots p^e)$，$\sigma_2=(\bar{1}\ \bar{2}\cdots\cdots\bar{p})$，设

$$E^*=\{〔1,2〕,〔1,\bar{1}〕,〔1,\bar{2}〕,〔1,\bar{4}〕\},\ E=E(G)=\bigcup_{1}^{p^e}\sigma^i(E^*)，则$$

$|E|=4p^e$，$\sigma\in\mathrm{Aut}G$。$V_1=V(\sigma_1)$中顶点的度都是5，$V_2=V(\sigma_2)$中的度都是$3p^{e-1}$，因此若$\tau\in\mathrm{Aut}G$，则τ不会把V_1中顶点变为V_2中顶点，因此$\tau=\tau_1\tau_2$，τ_i是τ在V_i上的限制。设$\tau=\tau_1\tau_2$，$\tau(1)=1$，因为$G_1=G(V_1)=1\ \ 2\cdots\cdots p^e\ 1$是一个圈，因此$\tau=\varepsilon_1$或$\tau_1=(1)(2p^e)(3p^e-1)\cdots\cdots$，设$\tau_1=(1)(2p^e)(3p^e-1)$，与1邻接的$V_2$中顶点集是$\{\bar{1},\bar{2},\bar{4}\}$，因此$\tau(\bar{2})\in\{\bar{1},\bar{2},\bar{4}\}$。与2和$p^e$邻接的$V_2$中点集分别是$\{\bar{2},\bar{3},\bar{5}\}$和$\{\bar{p},\bar{1},\bar{3}\}$，因此$\tau(\bar{2})\in\{\bar{p},\bar{1},\bar{3}\}$，$\tau(\bar{2})=\bar{1}$。与$p^e-1$和3邻接的$V_2$中点集分别是$\{\overline{p-1},\bar{p},\bar{2}\}$和$\{\bar{3},\bar{4},\bar{6}\}$，因此$\tau(\bar{2})\in\{\bar{3},\bar{4},\bar{6}\}$，矛盾，因此$\tau_1=\varepsilon_1$，由此易知$\tau_2=\varepsilon_2$，$\tau=\varepsilon$。设$\tau(1)=1+i$，则$\sigma^{-i}\tau(1)=1$，$\sigma^{-i}\tau=\varepsilon$，$\tau=\sigma^i$，即AutG中任意元是$\sigma$的幂，因此$\mathrm{Aut}G=(\sigma)$，这就证明了$\alpha(p^e)=p^e+p$（系3），也证明了$\beta(p^e)\leqslant 4p^e$。下面要证$\beta(p^e)\geqslant 4p^e$。设$\mathrm{Aut}G=(\sigma)$是$p^e$阶群，G有$p^e+p$个顶点。由前面的证明知$\sigma$是一个长为$p^e$和一个长为p的轮换之积。设$\sigma=\sigma_1\sigma_2$，$\sigma_1$，$\sigma_2$，$V_1$，$V_2$等与前面相同。设1与$V_2$中a个顶点邻接，则$V_1$中任意顶点都与$V_2$中a个顶点邻接。设$E_{12}$是一个顶点在$V_1$另一个$V_2$在的边的集合，则$|E_{12}|=ap^e$。设$\tau_1=(1)(2p^e)(3p^e-1)\cdots\cdots$，$\tau_2=(\bar{i})(\overline{i-1}\ \ \overline{i+1})(\overline{i+2}\ \ \overline{i-2})\cdots\cdots$，$\tau_3=(\bar{i}\ \ \bar{j})(\overline{i-1}\ \ \overline{j+1})(\overline{i-2}\ \ \overline{j+2}\cdots\cdots)$。设$a=0$，则易证$\tau_1\in\mathrm{Aut}G$，矛盾，设$a=1$，1与$\bar{i}$邻接，则易证$\tau_1\tau_2\in\mathrm{Aut}G$，矛盾，设$a=2$，1与$\bar{i}$，$\bar{j}$邻接，则易证$\tau_1\tau_3\in\mathrm{Aut}G$，矛盾，因此$a\geqslant 3$，$|E_{12}|\geqslant 3p^e$。用$E_i$表示两个顶点都在$V_i$中的边的集。设$e>1$，若$|E_1|=0$，即$V_1$中任意两点都不邻接，则易证$(1\ \ p+1)\in\mathrm{Aut}G$，矛盾。设〔i,j〕$\in E_1$，则$\sigma^x$〔i,j〕$\in E_1$ $(x=1,2,\cdots\cdots,p^e)$，因此$|E_1|\geqslant p^e$，$|E(G)|\geqslant|E_1|+|E_{12}|\geqslant 4p^e$。设$e=1$，$|E_1|+|E_2|=0$，则易证$(1\ \bar{1})(2\ \bar{p})(3\ \overline{p-1})\cdots\cdots(p\ \bar{2})\in\mathrm{Aut}\,G$，矛盾，因此$|E_1|+|E_2|\geqslant p$，$|E(G)|\geqslant 4p$。　　证毕

系4　$\alpha(p^e)=p^e+p$　$(p\geqslant 7)$

系5　设$\mathrm{Aut}\,G=(\sigma)$，$\sigma=(1\ \ 2\cdots\cdots m)\ (\bar{1}\ \ \bar{2}\cdots\cdots\bar{n})$，$m=kn$，则$|E(G)|\leqslant$

中国知网 https://www.cnki.net

$4m$。

引理 2　设$n=p_1^{e_1}p_2^{e_2}\cdots\cdots p_r^{e_r}$，（$p_i\geqslant 7$，$i=1$，2，……，r），$r(n)=\sum\limits_1^r(p_i^{e_i}+p_i)$，则$\alpha(n)\leqslant r(n)$，$\beta(C_n, r(n))\leqslant 4\sum\limits_{i=1}^r p_i^{e_i}$。

证明　设G有r个支G_i，（i＝1，2，……，r），Aut G_i是$p_i^{e_i}$阶群，G_i有$p_i^{e_i}+p_i$个顶点，$4p_i^{e_i}$条边。易知Aut G是n阶群，因此$\alpha(n)\leqslant r(n)$，$\beta(C_n, r(n))\leqslant 4\sum\limits_1^r p_i^{e_i}$。

下面的引理3是易证的。

引理 3　设n与引理2的相同，$T=\{p_1^{e_1}, p_2^{e_2}\cdots\cdots p_j^{e_j}, n_1, n_2, \cdots\cdots, n_k\}$，$1\leqslant j+k\leqslant r$，n是T中$j+k$个数的最小公倍数，$n_i$不是素数幂（i＝1，2，……，k）。设$p_1$，$p_2$，……，$p_x$都与$n_i$（i＝1，2，……k）互素，$p_y$（$x<y\leqslant j$）总与某个$n_i$不互素，则T中$j+k$个数之和$\geqslant r(n)-(p_1+p_2+\cdots\cdots+p_x)$，当且仅当$x=r$，$k=0$时等号成立。

引理 4　设n与引理2的相同，则$\alpha(n)=r(n)=\sum\limits_1^r(p_i^{e_i}+p_i)$。

证明　由引理2，只要证$\alpha(n)\geqslant r(n)$。设Aut G＝（σ）是n阶群，$\sigma=\sigma_1\sigma_2\cdots\cdots\sigma_z$，$S=\{\sigma_1, \sigma_2, \cdots\cdots\sigma_z\}$。设$H_i=\{\tau\mid\tau\in S, |\tau|$是$p_i^{e_i}$的倍数$\}$，因为n是S中轮换长的最小公倍数，因此$H_i$非空（i＝1，2，……，r）。设$T^1=\{\tau_1, \tau_2, \cdots\cdots, \tau_r\}$，$\tau_i\in H_i$，$T^1$中轮换可能有相同的，因此实际上$T^1=\{\tau_1, \tau_2, \cdots\cdots, \tau_{j+k}\}$（$1\leqslant j+k\leqslant r$）。设$T=\{|\tau_1|, |\tau_2|, \cdots\cdots, |\tau_{j+k}|\}$，则T是引理3中的那种数的集合；这些数的和$\geqslant r(n)-(p_1+p_2+\cdots\cdots+p_x)$。设$|\tau_1|=p_1^{e_1}$即$\tau_1$的长度与$T^1$中其它轮换的长度都互素，根引理1，存在$\tau\in S$，$\tau\notin T'$，$|\tau_1|$与$|\tau|$不互素；即$|\tau|=w_1p_1$，对于i＝1，2，……，$x_1$都存在$\tau_i'\in S$，$\tau_i'\notin T'$，使得$|\tau_i'|=w_ip_i$，易证S的不在$T'$中的轮换长度之和$\geqslant p_1+p_2+\cdots\cdots+p_x$，因此$|V(G)|\geqslant r(n)$，$\alpha(n)\geqslant r(n)$。

系 6　设n与引理2的相同，Aut G＝（σ）是n阶群，G有α(n)个顶点，则$\sigma=\sigma_1\overline{\sigma_1}\sigma_2\overline{\sigma_2}\cdots\cdots\sigma_r\overline{\sigma_r}$，$|\sigma_i|=p_i^{e_i}$，$|\overline{\sigma_i}|=p_i$（i＝1，2，……，r）。

定理2的证明，由引理2，只要证$\beta(n)\geqslant 4\sum\limits_1^r p_i^{e_i}$。设Aut G＝（σ）是n阶群，G有α(n)个顶点。设σ与系6的相同，设$V_1=V(\sigma_1\overline{\sigma_1})$，$\sigma_1=(1\ \ 2\cdots\cdots p_1^{e_1})$，$\overline{\sigma_1}=(\overline{1}\ \ \overline{2}\cdots\cdots\overline{p_1})$，$G_1=G(V_1)$，$E_1$是一个顶点在$V(\sigma_1)$另一个在$V(\overline{\sigma_1})$的边的集。设$d\notin V_1$，由引理1的证明可知若d与$V(\sigma_1)$（$V(\overline{\sigma_1})$）中一个顶点邻接，则d与$V(\sigma_1)$（$V(\overline{\sigma_1})$）中所有顶点邻接。这样，若$\tau\in$ Aut G_1，τ不把$V(\sigma_1)$中顶点变为$V(\overline{\sigma_1})$中顶点，则$\tau\in$ Ant G。

中国知网 https://www.cnki.net

如同定理1证明那样，可证 $|E_1| \geqslant 3p_1^{e_1}$，若 $e_1 > 1$，则 $|E(G(V(\sigma_1)))| \geqslant p_i^{e_i}$。设 $e_1 = 1$，$G(V(\sigma_1))$ 和 $G(V(\overline{\sigma_1}))$ 中有一个不是零图（任意两点都不邻接的图），则 $|E(G_1)| \geqslant 4p_1$。设2个都是零图，V_1 的顶点与不在 V_1 中的顶点都不邻接，则 $(1\ \overline{1})(2\ \overline{p_1})\cdots\cdots(p_1\ \overline{2}) \in \mathrm{Aut}\,G$，矛盾。设1与 $V(\overline{\sigma_i})$ 中的顶点邻接，则 $V(\overline{\sigma_1})$ 中所有顶点与 $V(\overline{\sigma_i})$ 中所有顶点都邻接，这样的边有 p_1p_i 条，把 $\left[\frac{p_1p_i}{2}\right]$ 条加到 $E(G_1)$ 中来计算，则

$|E(G_1)| \geqslant 4p_1$，同样 $|E(G_i)| \geqslant 4p_i^{e_i}$ $(i = 1, 2, \cdots\cdots, r)$，因此 $|E(G)| \geqslant 4\sum_1^r p_i^{e_i}$，

$\beta(n) \geqslant 4\sum_1^r p_i^{e_i}$。　　证毕

参考文献

〔1〕Harary, F., and Palmer, E. M, The smallest graph whose group is cyclic, Czech. Math. J. 16 (1966), 70—71。Math Reviews, 33 (1967) #2563。

〔2〕Sabidussi, G., On the minimum order of graphs with given automorphism group, Monatsh. Math. 63 (1959), 124—127。

〔3〕Frucht, R., Graphs of degree 3 with given abstract group, Canad. J. Math. 1 (1949), 365—378。

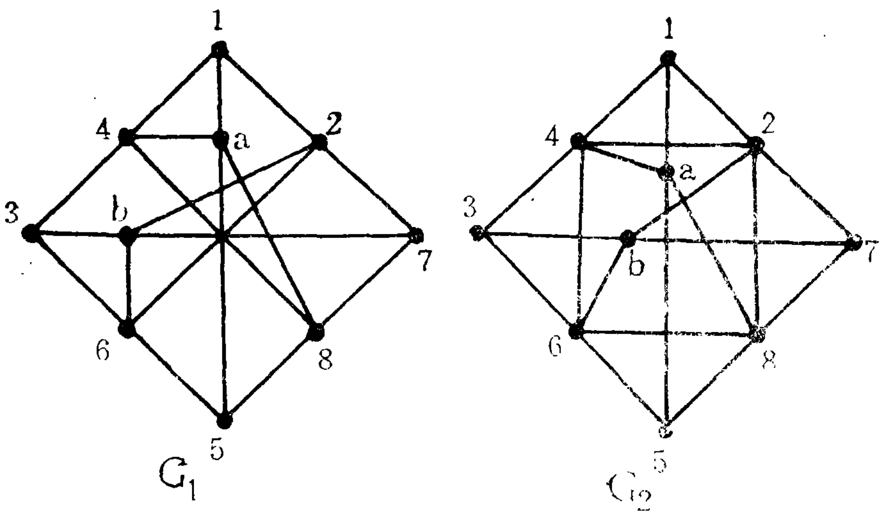
〔4〕Harary, F., Graph theory, Addison-Whesley, 1969，中译本，图论，李慰萱译，上海科学技术出版社，1980年。

中国知网 https://www.cnki.net

二、循环群C_4的最小图

任给n阶有限群F_n，Frucht，R构造出自同构群与F_n同构的图（〔1〕，194—196），但这种图具有较多的顶点。具有给定群且顶点或边数最小的图被许多作者研究过。Meriwether给出了具有与C_n的群同构的群的图的最少顶点数C(n)（〔1〕，203）但没有发表。当p是素数时，Sabidussi构造出C_p的顶点最少的图（〔2〕），他的C_3和C_5的图分别具有18和30条边。Harary和Palmer构造的C_3和C_5的图分别有15和25条边③，并且这是边的最小数目，他们也构造了C_4的图，具有12个顶点和20条边。Meriwether的C_4的图有10个顶点和20条边④。1969年Frucht在给Qlutas的未发表的私人通信中说：一定存在10个顶点，18条边的C_4的图④。我们构造出自同构群为C_4且顶点最少的图，其中边数最少的是18条边。根据Meriwether的公式，C(4)=10。这12个图的顶点集都用V表示，V={1，2，3，4，5，6，7，8，a，b，}，我们用f=(1357)(2468)(ab)表示V上的一个置换，由f生成的群用(f)表示。这12个图用G_i和$\overline{G_i}$表示(i=1，2，……，6，)，这里$\overline{G_i}$是G_i的补图，它们的自同构群都是(f)，我们仅对G_1进行证明，其它几个的证明是类似的。图1给出了G_1和G_2。

图 1



G_1的群是(f)的证明。易知f=(1357)(2468)(ab)是G_1的自同构。奇数顶点的度是3，其它顶点的度都是4，因此若h是G_1的自同构，则h(i)∈{1，3，5，7}，{i=1，3，5，7}。与2邻接的顶点集{1，7，b，6}以及2这5个顶点的导出子图具有6条边，与a邻接的顶点集{1，4，5，8}以及a这5个顶点的导出子图具有7条边，因此h(i)∈{2，4，6，8}，(i=2，4，6，8)，h{a，b}={a，b}。h(1)=1 ⟹ h(a)=a ⟹ h(2)=2，h(4)=4。h(2)=2 ⟹ h(b)=b，h(6)=6。h(4)=4 ⟹ h(8)=8。最后h(3)=3，h(5)=5，h(7)=7，因此h=e是恒等置换，即由h(1)=1可推出h=e。设h(1)=1+i，则$f^{-i}h(1)=1$，于是$f^{-i}h=e$，$h=f^i$，即群中任意元素是f的幂，因此G_1的群是(f)。 证毕

图2给出G_3，G_4，G_5，G_6。用E_i表示G_i的边数，我们有$E_1=18$，$E_2=20$，$E_3=19$，$E_4=21$，$E_5=E_6=22$。G_5和G_6的顶点的度序列分别是（3，3，3，3，4，4，6，6，6，

中国知网 https://www.cnki.net

6）和（4，4，4，4，4，4，5，5，5，5），因此这6个图是互不同构的。$\overline{G_i}$（i＝1，2，……，6）的边的数都大于22，因此这一共12个图是互不同构的。

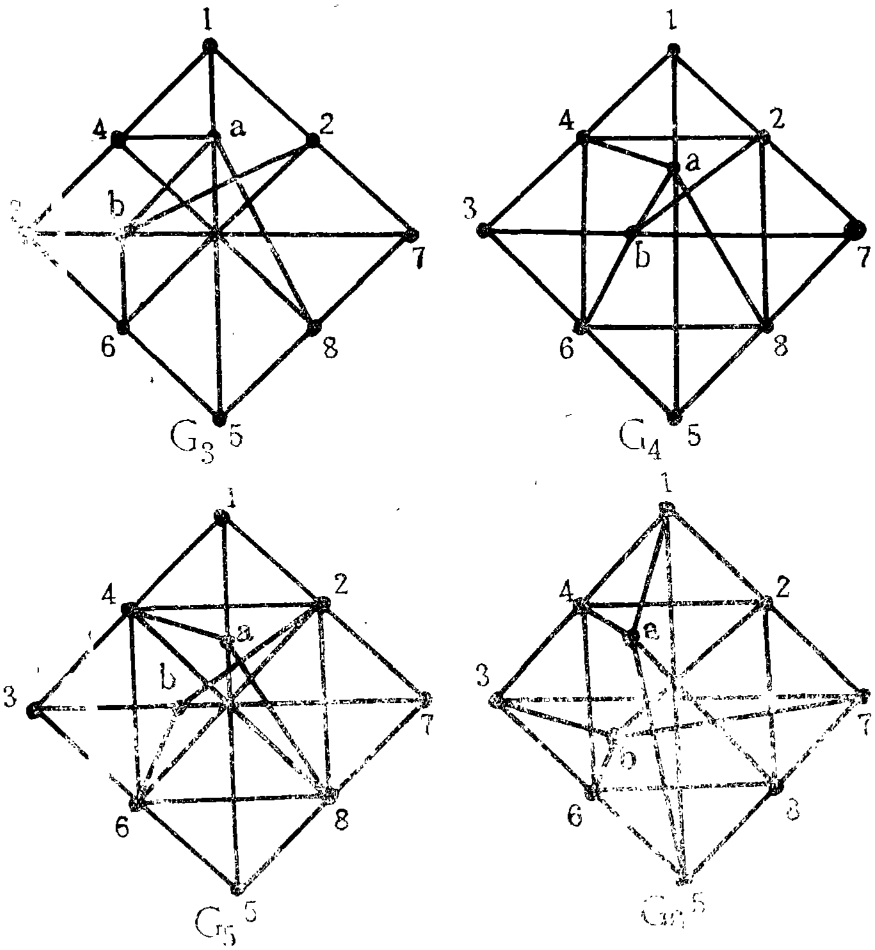


图 2

本文得到中国科技大学李乔老师的关怀和帮助，在此表示感谢。

参 考 文 献

①Harary，F，Graph theory，Addison－Wesley，1969 中译本图论，李慰萱译，上海科学技术出版社，1980年。

②Sabidussi，G，On the minimum order of graphs with given automorphism group，Moatnsh．Math．63（1959），124—127

③Harary，F，and Palmer，E．M．，The smallest graph whose group is cyclic，Czech．Math．J．16（1966）70—71

④Allan Gewirtz，Anthony Hill and Louis V．Quintas，Extremum Problems Concerning graphs and their Groups，Combinatorial structures and Their Applications，1970

中国知网 https://www.cnki.net

On The Smallest Graph Whose Group Is Cyclic

Zhou Shang chao

East China Jiaotong University, Nanchang

Abstract

Let $\alpha(n)$ be the least number of vertices for which a graph has automorphism group isomorphic to c_n, the cyclic group of orber n. Let $\beta(c_n,\alpha(n))$ represent the least number of edges a graph can have if it has $\alpha(n)$ vertices and automorphism group isomorphic to c_n. Then the following theorem is obtained.

Theorem. (1) $\beta(c_n,\alpha(n))=4n$, $n=p^e$, $p\geqslant 7$, p is prime.

(2) Let $n=p_1^{e_1}p_2^{e_2}\cdots\cdots p_r^{e_r}$ be the prime decomposition of n, $p_i\geqslant 7$ $(i=1, 2, \cdots\cdots, r)$, Then $\beta(c_n,\alpha(n))=4\sum\limits_{1}^{r}p_i^{e_i}$.

中国知网 https://www.cnki.net