第 14 卷第 1 期　常德师范学院学报(自然科学版)　Vol. 14 No. 1
2002 年 3 月　Journal of Changde Teachers University(Natural Science Edition)　Mar. 2002

文章编号: 1009- 3818(2002)01- 0007- 02

一个幂指不等式及其应用

倪仁兴　张森国
(绍兴文理学院 数学系　浙江 绍兴　312000)

摘　要: 幂指不等式在数学竞赛中时有出现, 其证明往往是比较困难的. 本文借助于新的分析技巧给出了一个新颖的幂指不等式(即任给两个正数 a 和 b, 有 $a^a + b^b$ 不小于 $a^b + b^a$)及其推广形式, 并将所得结果应用于一数学竞赛题的证明中.

关键词: 幂指不等式; 数学归纳法; 增函数; 置换
中图分类号: O 178　文献标识码: A

不等式的求解和证明在数学竞赛中是经常出现的, 而幂指不等式的证明往往比较难且在竞赛中也时有出现. 常见的幂指不等式中有 $a^a \cdot b^a \geqslant a^b \cdot b^a$(其中 a 和 b 为两正数)(见文献[2])等这样的不等式, 由此自然联想到 $a^a + b^a \geqslant a^b + b^a$, 其中 a 和 b 为两正数的不等式是否成立? 本文先给这个问题以肯定的回答并作了相应的推广(分别见下面的定理 1 和定理 2), 后举例说明其应用.

引理 1　1) 设 $a \geqslant b > 0$ 且 $a \geqslant 1$, 则函数 $F(u) = a^u - b^u$ 在 $(0, +\infty)$ 上为 u 的不减函数.

2) 设 $1 \geqslant a \geqslant b > e^{-1}$, 则函数 $F(u) = a^u - b^u$ 在 $(e^{-1}, 1]$ 上为 u 的不减函数.

证明　用一般的分析方法可证

注 1　当 $a, b \in (0, e^{-1})$ 时, $F(u)$ 在 $(0, e^{-1})$ 上一般不是单调函数. 如

1) 取 $a = 0.000\,2$, $b = 0.000\,1$, $u_1 = 0.2$, $u_2 = 0.3$
　则有 $F(u_1) > F(u_2)$

2) 取 $a = 0.02$, $b = 0.01$, $u_1 = 0.15$, $u_2 = 0.016$
　则有 $F(u_1) < F(u_2)$.

定理 1　设 $a, b > 0$, 则 $a^a + b^b \geqslant a^b + b^a$

证明　根据对称性不妨设 $a \geqslant b$, 当 $a \geqslant b > 0$ 且 $a \geqslant 1$ 时, 由引理 1 可得 $a^a - b^a \geqslant a^b - b^b$ 即: $a^a + b^b \geqslant a^b + b^a$, 下证当 $0 < b \leqslant a \leqslant 1$ 时 $g(z) = a^a - a^z - (z^a - z^z)$ 在 $(0, a]$ 上非负, 事实上, 由

$$
\begin{aligned}
g'(Z) &= -a^Z \cdot \ln a - a \cdot Z^{a-1} + Z^Z \cdot (1 + \ln Z) \\
&= (Z^Z \cdot \ln Z - a^Z \cdot \ln a) + (Z^Z - a \cdot Z^{a-1}) \\
&= -\int_Z^a \frac{\mathrm{d}}{\mathrm{d}S}(S^Z \cdot \ln S)\,\mathrm{d}S + (Z^Z - a \cdot Z^{a-1}) \\
&= -\int_Z^a S^{Z-1} \cdot (1 + Z \cdot \ln S)\,\mathrm{d}S + (Z^Z - a \cdot Z^{a-1})
\end{aligned}
$$

令 $f(Z) = Z \cdot \ln Z$, 易知 $\inf_{Z \in (0, +\infty)} f(Z) = -e^{-1}$, 注意到 $Z \in (0, 1]$, $Z \cdot \ln Z \geqslant -e^{-1}$, 这样当 $0 < Z \leqslant S \leqslant a \leqslant 1$ 时 $1 + Z \cdot \ln S \geqslant 1 + Z \cdot \ln Z \geqslant 1 - e^{-1} \geqslant 0$, 得 $-\int_Z^a S^{Z-1} \cdot (1 + Z \cdot \ln S)\,\mathrm{d}S \leqslant 0$. 记 $h(Z) = Z^Z - a \cdot Z^{a-1}$, 下证 $h(Z) < 0$, $\forall Z \in (0, a)$. 作函数 $\varphi(S) = Z^Z - S \cdot Z^{S-1}$ ($S \in (0, +\infty)$) 则 $\varphi(Z) = 0$, $\varphi(a) = h(Z)$, 下只要证 $\varphi(a) < 0$. 事实上若 $\varphi(a) \geqslant 0$, 则由于 $\varphi(Z) = 0$ (当 $Z \in (0, a)$) 而在 $[a, 1)$ 上, $\varphi(1) = Z^Z - 1 = e^{Z \cdot \ln Z} - 1 < 0$. 因 $\phi'(S) = -Z^{S-1}(1 + S\ln Z)$ 在 $(0, +\infty)$ 只有唯一的零点 $S = -\dfrac{1}{\ln Z}$, 根据罗尔定理, $\phi(S)$ 在 $(0, +\infty)$ 至多有两个零点. 已知 $S = Z \in (0, a)$ 为其一个零点, 又 $\phi(1) = Z^Z - 1 < 0$ ($\because Z < 1$) $\lim_{S \to +\infty} \phi(S) = Z^Z > 0$ 故在 $(1, +\infty)$ 间还有一个零点, 所以当 $a \leqslant s \leqslant 1$ 时, 再无零点, $\phi(a)$ 必与 $\phi(1)$ 同号, 故 $\varphi(a) < 0$, 即 $h(Z) < 0$, 这样 $g'(Z) < 0$, $Z \in (0, a)$, 即 $g(Z)$ 在 $(0, a)$ 上是严格单调递减, 故 $\forall Z \in (0, a]$ 有 $g(Z) \geqslant g(a) = 0$, 这样 $g(b) \geqslant g(a) = 0$, 即 $a^a + b^b \geqslant a^b + b^a = 0$, 证毕.

引理 2　设 $e^{-1} < a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n$, 则

$$
a_1^{a_2} + a_2^{a_3} + \cdots + a_{n-1}^{a_n} + a_n^{a_1} \leqslant a_1^{a_1} + a_2^{a_2} + \cdots + a_n^{a_n} \tag{1}
$$

证明　下面用数学归纳法证明.

当 $n = 2$ 时利用定理 1 可得 $a_1^{a_2} + a_2^{a_1} \leqslant a_1^{a_1} + a_2^{a_2}$ 成立. 假设 $n = k - 1$ 时也成立, 即: $a_1^{a_2} + a_2^{a_3} + \cdots + a_{k-2}^{a_{k-1}} + a_{k-1}^{a_1} \leqslant a_1^{a_1} + a_2^{a_2} + \cdots + a_{k-1}^{a_{k-1}}$ 成立. 当 $n = k$ 时, 两边加 $a_k^{a_k}$ 即得下式:

收稿日期: 2001- 07- 17
修回日期: 2001- 09- 25
第一作者: 倪仁兴(1964-) 男 副教授 硕士
国家自然科学基金资助项目(19971013)
浙江省高校中青年学科带头人基金资助项目

$a_1^{a_2}+a_2^{a_3}+\cdots+a_{k-2}^{a_{k-1}}+a_{k-1}^{a_1}+a_k^{a_k}\leqslant a_1^{a_1}+a_2^{a_2}+\cdots+a_{k-1}^{a_{k-1}}+a_k^{a_k}$;

而由引理1有 $a_k^{a_k}-a_{k-1}^{a_k}\geqslant a_k^{a_1}-a_{k-1}^{a_1}$ 即: $a_k^{a_k}+a_{k-1}^{a_1}\geqslant a_k^{a_1}+a_{k-1}^{a_k}$ 故 $a_1^{a_1}+a_2^{a_2}+\cdots+a_k^{a_k}\geqslant a_1^{a_2}+a_2^{a_3}+\cdots+a_{k-2}^{a_{k-1}}+a_{k-1}^{a_1}+a_k^{a_k}\geqslant a_1^{a_2}+a_2^{a_3}+\cdots+a_{k-1}^{a_k}+a_k^{a_1}$, 证毕.

定理2 设 $e^{-1}<a_1\leqslant a_2\leqslant\cdots\leqslant a_n$, $i_1, i_2, \cdots, i_n$ 是1, 2, …, n 的一个置换, 则 $\sum_{k=1}^{n}a_k^S\leqslant\sum_{k=1}^{n}a_k^t$ $(S=a_{j_k};t=a_k)$

证明 只要对引理2中(1)的左边部分 $a_1^{a_2}+a_2^{a_3}+\cdots+a_{n-1}^{a_n}+a_n^{a_1}$ 记为 I_n, 现让 I_n 中的幂指数任意交换一次, 不妨设幂指数 a_i 和 a_j 对换, 且 $a_i\geqslant a_j$, 此时 I_n 变为下式:

$$a_1^{a_2}+a_2^{a_3}+\cdots+a_{i-1}^{a_j}+\cdots+a_{j-1}^{a_i}+\cdots+a_{n-1}^{a_n}+a_n^{a_1}\qquad(2)$$

记为 T_n, 下面只要证明 $T_n\leqslant I_n$ 就可以了, 事实上由引理1可得

$a_{i-1}^{a_i}-a_{j-1}^{a_i}\geqslant a_{i-1}^{a_j}-a_{j-1}^{a_j}$ 即: $a_{i-1}^{a_i}+a_{j-1}^{a_j}\geqslant a_{j-1}^{a_j}+a_{j-1}^{a_i}$;

故 $T_n\leqslant I_n$ 得证. 以下只要对(1)式做同上类似的置换, 反复用引理1的结论即可, 这样由引理2可得 $\sum_{k=1}^{n}a_k^S\leqslant\sum_{k=1}^{n}a_k^t$ $(S=a_{i_k};t=a_k)$ 成立.

注2 当 $0<a_k<e^{-1}$ 时 $(k=1, 2, \cdots, n)$ 定理2的结论一般不成立. 如

1) 取 $a_{i-1}=0.000\ 2$, $a_{j-1}=0.000\ 1$, $a_j=0.2$, $a_i=0.3$

则有 $T_n>I_n$.

2) 取 $a_{i-1}=0.02$, $a_{j-1}=0.01$, $a_j=0.015$, $a_i=0.016$

则有 $T_n<I_n$.

推论 设 $e^{-1}<a_1\leqslant a_2\leqslant\cdots\leqslant a_n$, $i_1, i_2, \cdots, i_n$ 与 $j_1, j_2, \cdots, j_n$ 是1, 2, …, n 的任意两个排列, 则:

$a_{i_1}^{a_{j_1}}+a_{i_2}^{a_{j_2}}+\cdots+a_{i_n}^{a_{j_n}}\leqslant a_1^{a_1}+a_2^{a_2}+\cdots+a_n^{a_n}$;

$a_{i_1}^{a_{j_1}}+a_{i_2}^{a_{j_2}}+\cdots+a_{i_n}^{a_{j_n}}\geqslant a_1^{a_n}+a_2^{a_{n-1}}+\cdots+a_n^{a_1}$.

证明 $a_{i_1}^{a_{j_1}}+a_{i_2}^{a_{j_2}}+\cdots+a_{i_n}^{a_{j_n}}\leqslant a_1^{a_1}+\cdots+a_n^{a_n}$ 由定理2直接可得. 下证 $a_1^{a_n}+a_2^{a_{n-1}}+\cdots+a_n^{a_1}$ 是这些置换中数值最小的一个就可以了. 对 $a_1^{a_n}+a_2^{a_{n-1}}+\cdots+a_n^{a_1}$ 的幂指数任意交换一次, 不妨设是幂指数 a_{n-i+1} 与 a_{n-j+1} 对换, 此时变成:

$$a_1^{a_n}+\cdots+a_i^{a_{n-j+1}}+\cdots+a_j^{a_{n-i+1}}+\cdots+a_n^{a_1}\qquad(3)$$

不妨设 $n\geqslant i\geqslant j\geqslant 1$, 由题设得 $a_{n-j+1}\geqslant a_{n-i+1}$, 再用引理1可得

$a_i^{a_{n-j+1}}-a_j^{a_{n-j+1}}\geqslant a_i^{a_{n-i+1}}-a_j^{a_{n-i+1}}$ 所以有下式 $a_1^{a_n}+a_2^{a_{n-1}}+\cdots+a_n^{a_1}\leqslant a_1^{a_n}+\cdots+a_i^{a_{n-i+1}}+\cdots+a_j^{a_{n-i+1}}+\cdots+a_n^{a_n}$

以下只要对 T_n 再进行类似的置换, 反复用引理1的结论即可, 证毕.

猜想 推论对任意满足 $0<a_1\leqslant a_2\leqslant\cdots\leqslant a_n$ 的数 a_i $(i=1, 2, \cdots, n)$ 也成立.

下面我们给出定理的一个应用.

例 设 $a=\frac{m^{m+1}+n^{n+1}}{m^m+n^n}$ 其中 $m, n\in N$, 则 $a^m+a^n\geqslant m^n+n^m$ (由1991年美国第20届数学奥林匹克竞赛题4改编, 见文献[1]).

证明: 不妨设 $m\geqslant n$, 则 $a\leqslant\frac{m\cdot m^m+m\cdot n^n}{m^m+n^n}=m$, $a\geqslant\frac{n\cdot m^m+n\cdot n^n}{m^m+n^n}=n$

故 $n\leqslant a\leqslant m$, 这样

$$\begin{aligned}m^m-a^m&=(m-a)\cdot(m^{m-1}+m^{m-2}\cdot a+\cdots+a^{m-1})\\&\leqslant(m-a)\cdot(m^{m-1}+m^{m-1}+\cdots+m^{m-1})\\&=(m-a)\cdot m^m\\a^n-n^n&=(a-n)\cdot(a^{n-1}+a^{n-2}\cdot n+\cdots+n^{n-1})\\&\geqslant(a-n)\cdot(n^{n-1}+n^{n-1}+\cdots+n^{n-1})\\&=(a-n)\cdot n^n\end{aligned}$$

而 $a=\frac{m^{m+1}+n^{n+1}}{m^m+n^n}$, 即 $(m-a)\cdot m^m=(a-n)\cdot n^n$

这样 $a^m+a^n\geqslant m^m+n^n$, 由定理可得 $a^m+a^n\geqslant m^n+n^m$, 证毕.

参 考 文 献

1 单 ,胡炳生, 胡礼祥, 等. 数学奥林匹克竞赛题解精编[M]. 南京: 南京大学出版社, 2000. 161.

2 匡继昌. 常用不等式(第2版)[M]. 长沙: 湖南教育出版社, 1993. 181.

3 杨学枝. 不等式研究[M]. 拉萨: 西藏人民出版社, 2000. 83-88. .

A POWER EXPONENT INEQUALITY AND ITS APPLICATION

NI Ren-xing ZHANG Sen-guo

(Dept. of Math. Shaoxing College of Arts and Sciences, Shaoxing Zhejiang, 312000)

Abstract Power exponent inequality often appeared in Mathematical Olympian,

(下转第18页)

由引理7, $N_f = 2^{n_2}N_{f_1} + 2^{n_1}N_{f_2} - 2N_{f_1}N_{f_2}$
因为线性函数 $u + v$ 的非线性度为0,
故 $N_f = 2^{n_2}N_{f_1} + 2^{n_1}N_{f_2} - 2N_{f_1}N_{f_2} = 2^2(2^{2k-1} - 2^{k-1}) = 2^{2k+1} - 2^{k+1}$.

证明完毕.

推论10 令 f 为 $n-m$ 元Bent函数, g 为 n 元布尔函数, $m < n$,
$g(x_1, \cdots, x_n) = x_1 + x_2 + \cdots + x_m + f(x_{m+1}, \cdots, x_n)$.

则 g 是平衡的, 并且除 $(\omega_1, \cdots, \omega_m, 0, \cdots, 0)$ 外, g 对任意的 n 维非零向量 λ 满足 n 次扩散准则. 其中 $\omega_1, \cdots, \omega_m \in Z_2$.

证明 $x_1 + \cdots + x_m$ 是线性函数, 故其是平衡的, 又由定理3, 显然 g 为平衡函数;

令 $\lambda = (a_1, a_2, \cdots, a_n) \notin \{(\omega_1, \cdots, \omega_m, 0, \cdots, 0)\}$, 其中 $\omega_1, \cdots, \omega_m \in Z_2$, $x = (x_1, x_2, \cdots, x_n)$. 则 $g(x) + g(x + \lambda) = a_1 + a_2 + \cdots + a_m + f(x_{m+1}, \cdots, x_n) + f(x_{m+1} + a_{m+1}, \cdots, x_n + a_n)$.

因为 f 为 $n-m$ 元Bent函数, 故 f 满足 $n-m$ 次扩散准则, 即对任意非零向量 $(a_{m+1}, \cdots, a_n)$, $f(x_{m+1}, \cdots, x_n) + f(x_{m+1}, + a_{m+1}, \cdots, x_n + a_n)$ 是平衡的.

于是, 对任意 n 维向量 $\lambda = (a_1, a_2, \cdots, a_n) \notin \{(x_1, \cdots, x_m, 0, \cdots, 0)\}$, $(x_1, \cdots, x_m \in Z_2)$, $g(x) + g(x + \lambda)$, 都是平衡的, 亦即除了 $\{x_1, \cdots, x_m, 0, \cdots, 0\}$, $(x_1, \cdots, x_m \in Z_2)$ 外, g 对任意 n 维非零向量 λ 满足 n 次扩散准则.

证明完毕.

参 考 文 献

1 O. S. Rothaus, On Bent Functions, J. [J]. of Combine Theory, 1976, 20(A), 300- 305.
2 J. Olsen, R. Scholtz and L. Welch, Bent Function Sequences[J]. IEEE Trans., 1982, IT- 28(6), 858- 864.
3 P. Kumar etal, Bounds on the linear span of Bent Sequences[J]. IEEE Trans., 1983, IT- 29(6), 854- 862.
4 R. Yarlagadda, J. Hershey, Analysis and Synthesis of Bent Sequences[J]. IEE Proc. (Part E.), 1989, 136(3), 112- 123.
5 C. Adams, S. Tavares, Generating and Counting Binary Bent Sequences[J]. IEEE Trans, 1990, IT- 36(5), 1 170- 1 173.
6 郭宝安, 蔡长年. 一类即非Bent基又非线性基的二元Bent序列的产生与计数[J]. 科学通报, 1991, 36(2): 810- 811.
7 武传坤. 布尔函数非线性度的谱分析[J]. 电子科学学刊, 1996, 18(5), 487- 495.
8 武传坤, 王新梅. 非线性置换的构造[J]. 科学通报, 1992, 37(12): 1 147- 1 151.
9 欧 洁, 罗铸楷. 关于Bent函数的一些研究[J]. 湘潭大学自然科学学报, 1999, 21(1): 7- 11.

THE RESEARCH ON BENT FUNCTION

QIU Xian- jie

(Department of Computer Science, Xiangtan University, Xiangtan Hunan, 411100)

Abstract Because of its the nonlinearity and stability, bent function have high value in the cryptogram theory. Because of its poor quantity and nonbalance, how to construct new bent function and how to apply bent function in new fields became a very significant problems. Some research on the construction and application of bent function was made. First, on the basis of literature 8 and 10, a new construction method of bent function by using boolean permutation that was the content of theorem 4 was put forward. In addition, according to the wide use of balance boolean functions with high nonlinearity in cryptogram theory, some research on this kind of functions was made. Two kinds of boolean functions satisfying the balancedness, the nonlinearity and the propagation criterion by using the characteristic of bent function and the conclusion of literature 8 about the nonlinearity of boolean function, which was the content of theorem 8 and 9 was put forward. So some new fields in the application of bent function were devoleped.

Key words boolean function; bent function; balance function; nonlinearity; propagation criterion

(责任编校: 魏承辉)

(上接第8页)

its proof was usually rather difficult. By virture of some new techniques of analysis, a novel power exponent inequality was given(If a and b are arbitrary two posstive numbers, then $a^a + b^b$ was no less than $a^b + b^a$), so was its extend. The results can also be applied to a Mathematical Olympian problem.

Key words power exponent inequality; mathemtics inductive methods; increasing function; exchange

(责任编校: 魏承辉)