Hence we have proved the

THEOREM. *If p is a prime greater than 3 there exist nontrivial morphisms of inequivalent extensions of Z_p by Z_p which are not isomorphisms.*

The author wishes to thank W. Messing for discussions which led to this note.

REFERENCE

1. J. J. Rotman, The Theory of groups, An Introduction, 3rd ed., Allyn and Bacon.

A Rearrangement Inequality and the Permutahedron

A. VINCE
Department of Mathematics, University of Florida, Gainesville, FL 32611

One chapter of the classic book "*Inequalities*" by Hardy, Littlewood, and Pólya [3] is dedicated to inequalities involving sequences with terms rearranged. The main example in that chapter is the following. Let $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n$ and $b_1 \leqslant b_2 \leqslant \cdots \leqslant b_n$ be sequences of real numbers and π any permutation of the set $\{1, 2, \ldots, n\}$. Then

$$\sum_{i=1}^{n} a_i b_{n-i+1} \leqslant \sum_{i=1}^{n} a_i b_{\pi i} \leqslant \sum_{i=1}^{n} a_i b_i. \tag{1}$$

Hardy, Littlewood, and Pólya interpret the a_i as fixed distances along a rod and the b_i as weights to be suspended at these distances: To get the maximum moment with respect to an end of the rod hang the heaviest weights furthest from that end; to get the minimum moment hang the heaviest weights closest.

Many variations and generalizations of this rearrangement inequality exist. Three appear below, more at the end of this note, and Marshall and Olkin [5] contains a relatively recent survey. In this note *all sequences* $\{a_i\}$ *and* $\{b_i\}$ *are increasing* in the sense $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n$ and $b_1 \leqslant b_2 \leqslant \cdots \leqslant b_n$, and *all sums and products are from* $i = 1$ *to* $i = n$ unless otherwise stated. Also $N = \{1, 2, \ldots, n\}$ and S_n denotes the set of all permutations of N.

Example 1. [7] For sequences with positive terms and for all $\pi \in S_n$

$$\prod(a_i + b_{n-i+1}) \geqslant \prod(a_i + b_{\pi i}) \geqslant \prod(a_i + b_i).$$

Example 2. [8] For $p \geqslant 1$ and all $\pi \in S_n$

$$\sum|a_i - b_i|^p \leqslant \sum|a_i - b_{\pi i}|^p \leqslant \sum|a_{n-i+1} - b_i|^p.$$

Example 3. [4] One generalization of the Hardy-Littlewood-Pólya inequality (1) is as follows. If the sequences have positive terms and f is an increasing convex function then for all $\pi \in S_n$

$$\sum f(a_i b_{n-i+1}) \leqslant \sum f(a_i b_{\pi i}) \leqslant \sum f(a_i b_i).$$

Recall that f is *increasing* if $f(x) \geqslant f(y)$ whenever $x \geqslant y$, and f is *convex* if

$f(\alpha x + (1 - \alpha)y) \leqslant \alpha f(x) + (1 - \alpha)f(y)$ for all $0 \leqslant \alpha \leqslant 1$. In the differentiable case, of course, convex is equivalent to $f''(x) \geqslant 0$.

The purpose of this note is to show how the permutahedron leads to a very simple generalization of the Hardy-Littlewood-Pólya inequality, from which the inequalities above and many other rearrangement inequalities immediately follow. In **[5]** rearrangement inequalities are derived using *majorization*, which is a partial order on the set of vectors in n-dimensional Euclidean space. This elegant method goes back at least to Schur **[10]** and is a unifying principal for many types of inequalities. The intention in this note is to use a much simpler partial order on S_n to obtain the rearrangement inequalities.

Let $\mathscr{I}$ denote the identity permutation $\mathscr{I}(i) = i$ of N and $\mathscr{I}_\star$ the reverse permutation $\mathscr{I}_\star(i) = n - i + 1, i = 1, \ldots, n$. An inversion of a permutation π of N is a pair $(\pi j, \pi k)$ such that $j < k$ and $\pi j > \pi k$. For example, $(5, 3)$ is one of the four inversions of $\pi = 2\,5\,1\,3\,4$. Now consider the directed graph P_n whose vertex set is S_n, and there is an edge (σ, π) directed from σ to π whenever vertex σ is obtained from vertex π by interchanging the elements of an inversion of the form $(\pi j, \pi(j + 1))$. P_n is sometimes called a permutahedron **[1]** and an example is shown in Figure 1. The transitive closure of P_n induces a partial order on the set S_n. Recall that the transitive closure is the "smallest" directed graph with the same vertex set as P_n and with the property that if (π, τ) and (τ, σ) are directed edges then so is (π, σ); the partial order on S_n is defined by $\sigma > \pi$ if there is an edge directed from σ to π in the transitive closure of P_n. A real valued function g: $S_n \to R$ is called *order preserving* if $g(\sigma) > g(\pi)$ whenever $\sigma > \pi$. This is all that is needed to prove the following theorem.

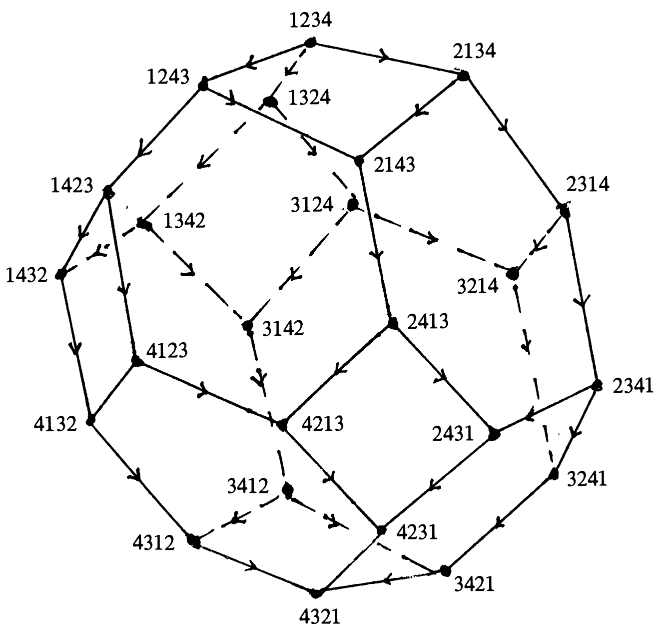

FIG. 1. Permutahedron P_4.

THEOREM. *Let $g_1, \dots, g_n$ be real valued functions defined on an interval I. Then*

$$\sum g_i(b_{n-i+1}) \leqslant \sum g_i(b_{\pi i}) \leqslant \sum g_i(b_i) \tag{2}$$

for all sequences $b_1 \leqslant b_2 \leqslant \cdots \leqslant b_n$ in I and all $\pi \in S_n$ if and only if

$$g_{i+1} - g_i \text{ is increasing on } I, \quad 1 \leqslant i < n. \tag{3}$$

Remark. If the functions g_i are differentiable, then it is clear that

$$g_1'(x) \leqslant g_2'(x) \leqslant \cdots \leqslant g_n'(x) \quad \text{for all } x \in I \tag{3'}$$

is equivalent to condition (3).

Proof. ($\Leftarrow$) Fix a sequence $b_1 \leqslant b_2 \leqslant \cdots \leqslant b_n$ and let $g\colon S_n \to R$ be defined by $g(\pi) = \sum g_i(b_{\pi i})$. To show that g is order preserving it suffices to show that $g(\sigma) > g(\pi)$ whenever (σ, π) is an edge of the permutahedron:

$$\begin{aligned} g(\sigma) - g(\pi) &= \left[g_j(b_{\sigma j}) + g_{j+1}(b_{\sigma(j+1)})\right] - \left[g_j(b_{\pi j}) + g_{j+1}(b_{\pi(j+1)})\right] \\ &= (g_{j+1} - g_j)(b_{\pi j}) - (g_{j+1} - g_j)(b_{\pi(j+1)}) \geqslant 0. \end{aligned}$$

The last inequality follows from $b_{\pi j} < b_{\pi(j+1)}$ and the assumption that $g_{j+1} - g_j$ is increasing. Since $\mathscr{I}_\star \leqslant \pi \leqslant \mathscr{I}$ for any permutation π, also $g(\mathscr{I}_\star) \leqslant g(\pi) \leqslant g(\mathscr{I})$, which is precisely inequality (2).

($\Rightarrow$) By way of contradiction assume that $g_{m+1} - g_m$ is not increasing for some m. Then there exists $x > y$ such that $(g_{m+1} - g_m)(x) < (g_{m+1} - g_m)(y)$. Now choose any sequence $b_1 \leqslant b_2 \leqslant \cdots \leqslant b_n$ in I with $b_m = x$ and $b_{m+1} = y$. Let π be the transposition $(m\ m+1)$. Then $\sum g_i(b_{\pi i}) =$

$$\begin{aligned} &\sum_{i \neq m,\, m+1} g_i(b_i) + g_m(x) + g_{m+1}(y) \\ &\quad > \sum_{i \neq m,\, m+1} g_i(b_i) + g_m(y) + g_{m+1}(x) = \sum g_i(b_i), \end{aligned}$$

contradicting inequality (2). □

The inequalities of Examples 1, 2, and 3, as well as those below, result by simply substituting the appropriate g_i in the theorem. For example, choosing $g_i(x) = a_i x$ yields the classic Hardy-Littlewood-Pólya inequality (1). Choosing $g_i(x) = -\log(a_i + x)$ yields Example 1; and choosing $g_i(x) = f(a_i x)$ gives Example 3. In each case it is an exercise to show that the g_i satisfy condition (3) or (3′) in the theorem. For the Hardy-Littlewood-Pólya inequality condition (3) is immediate. For Example 3 the verification of condition (3) is a little tricky, but still elementary.

Example 4. Let $g_i(x) = f(a_i - x)$. If f is convex then for all $\pi \in S_n$

$$\sum f(a_i - b_i) \leqslant \sum f(a_i - b_{\pi i}) \leqslant \sum f(a_{n-i+1} - b_i).$$

With $f(x) = |x|^p$ this is Example 2.

Example 5. [2] Take $g_i(x) = g(a_i, x)$ where g is a real valued function of two variables defined on a domain $D = [a, b] \times [c, d]$. If

$$g(x_1, y_1) - g(x_1, y_2) - g(x_2, y_1) + g(x_2, y_2) \geqslant 0 \tag{4}$$

for all $x_1 \geqslant x_2$, $y_1 \geqslant y_2$ in the domain then

$$\sum g(a_1, b_{n-i+1}) \leqslant \sum g(a_i, b_{\pi i}) \leqslant \sum g(a_i, b_i) \tag{5}$$

for all $\pi \in S_n$. Note that for a function with continuous second derivatives condition (4) can be replaced by

$$\frac{\partial^2 g(x, y)}{\partial x \partial y} \geqslant 0 \quad \text{for all}\,(x, y) \in D. \tag{4$'$}$$

Example 6. Many inequalities can be generalized to more than two sequences. Let $\{a_i^1\}$, $\{a_i^2\}, \dots, \{a_i^m\}$, $1 \leqslant i \leqslant n$, be *not necessarily increasing* real sequences and let $a_{(1)}, a_{(2)}, \dots, a_{(n)}$ denote the sequence $a_1, a_2, \dots, a_n$ in increasing order. Suppose $g(x_1, \dots, x_m)$ satisfies condition (4) or (4′) for every pair of variables. Then

$$\sum g\left(a_i^1, a_i^2, \dots, a_i^m\right) \leqslant \sum g\left(a_{(i)}^1, a_{(i)}^2, \dots, a_{(i)}^m\right). \tag{6}$$

This inequality follows directly by induction using the right inequality of (5) as the first step. Choosing $g(x_1, \dots, x_m) = x_1 x_2 \cdots x_m$ and $g(x_1, \dots, x_m) = -\log(x_1 + \cdots + x_m)$, respectively, in (6) results, for sequences of positive terms, in inequalities analogous to (1) and Example 2 [**9**]:

$$\sum a_i^1 a_i^2 \dots a_i^m \leqslant \sum a_{(i)}^1 a_{(i)}^2 \cdots a_{(i)}^m$$

and

$$\prod\left(a_i^1 + a_i^2 + \cdots + a_i^m\right) \geqslant \prod\left(a_{(i)}^1 + a_{(i)}^2 + \cdots + a_{(i)}^m\right).$$

Example 7. Choose $g(x_1, \dots, x_m) = f[\min(x_1, \dots, x_m)]$ in (6). If f is an increasing function then

$$\sum f\left(\min_j a_i^j\right) \leqslant \sum f\left(\min_j a_{(i)}^j\right).$$

Taking $f(x) = x$ and $f(x) = \log(x)$, respectively, leads to inequalities of Minc [**6**]:

$$\sum \min_j a_i^j \leqslant \sum \min_j a_{(i)}^j$$

and

$$\prod \min_j a_i^j \leqslant \prod \min_j a_{(i)}^j.$$

Similar inequalities hold for the max function.

REFERENCES

1. C. Berge, Principles of Combinatorics, Academic Press, New York and London, 1971.
2. P. W. Day, Rearrangement inequalities, *Canad. J. Math*, 24 (1972) 930–943.
3. G. H. Hardy, J. E. Littlewood, and G. Pólya, Inequalities, Cambridge University Press, London, 1952.
4. D. London, Rearrangement inequalities involving convex functions, *Pacific J. Math.*, 34 (1970) 749–753.
5. A. W. Marshall and I. Olkin, Inequalities: Theory of Majorization and Its Applications, Academic Press, New York, 1979.
6. H. Minc, Rearrangements, *Trans. Amer. Math. Soc.*, 159 (1971) 497–504.

7. A. Oppenheim, Inequalities connected with definite Hermitian forms II, *Amer. Math. Monthly*. 61 (1954) 263–266.
8. Y. Rinott, Multivariate majorization and rearrangement inequalities with some applications to probability and statistics, *Israel J. Math.*, 15 (1973) 60–77.
9. H. D. Ruderman, Two new inequalities, *Amer. Math. Monthly*, 59 (1952) 29–32.
10. I. Schur, Uber eine Klasse von Mittelbildungen mit Anwendungen die Determinanten, Theorie Sitzungsber., *Berlin. Math. Gesellschaft*, 22 (1923) 9–20.

Musings on the Prime Divisors of Arithmetic Sequences

PATRICK MORTON
Department of Mathematics, Wellesley College, Wellesley, MA 02181

Of the early proofs one usually sees in a number theory course, the most beautiful is the proof, due to Euclid, that there are infinitely many primes. This theorem may be formulated as follows.

If $\{a_n\}_{n=1}^{\infty}$ is any sequence of integers, and p is a prime for which $p|a_n$ for some n, p is called a *prime divisor* of the sequence $\{a_n\}_{n=1}^{\infty}$. (See **[2]**.) Euclid's theorem says that the sequence $\{n\}_{n=1}^{\infty}$ has an infinite set of prime divisors. What other sequences have this property?

For example, consider the sequences whose terms are defined by the following formulas:

1) $a_n = f(n)$, where $f \in \mathbf{Z}[x]$ is a nonconstant polynomial;
2) $b_n = [\pi n^2]$, where brackets denote the greatest integer;
3) $c_n = [\pi n^2]^2 - [\pi n^2]\left[\frac{\sqrt{2}}{en}\right] + \left[\frac{\sqrt{2}}{en}\right]^2$;
4) $d_n = 2^n + 1$.

Which of these sequences has an infinite number of prime divisors?

The answer is, of course, that they all do. The fact that $\{a_n\}_{n=1}^{\infty}$ does was first proved in an elementary way by Schur **[8]**, and is usually stated as follows. (See **[2]** and **[3]** for other proofs and more on the prime divisors of polynomials.)

THEOREM 1. *Let $f(x) \in \mathbf{Z}[x]$ be nonconstant. Then the congruence*

$$f(x) \equiv 0 (\mathrm{mod}\ p)$$

has a solution $x \in \mathbf{Z}$ for infinitely many primes p. In other words, infinitely many primes divide the terms of the sequence $\{f(n)\}_{n=1}^{\infty}$.

The purpose of this note is to give a surprising proof of this result using a well-chosen infinite series, and then to see where the proof leads. It will turn out that the proof can be generalized to show that the sequences $\{b_n\}_{n=1}^{\infty}$ and $\{c_n\}_{n=1}^{\infty}$ both have infinite sets of prime divisors, but that the same proof cannot decide this question for the simpler sequence $\{d_n\}_{n=1}^{\infty}$! The proof will also be a surprise in that it hides an algebraic structure.

1. A proof of Schur's theorem. Assume theorem 1 is false for some non-constant $f(x) \in \mathbf{Z}[x]$, and let $m = \deg f$. Then for $n \in \mathbf{Z}$, $f(n) = 0$ or (by the fundamental theorem of arithmetic)

$$f(n) = \pm p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$