PACIFIC JOURNAL OF MATHEMATICS
Vol. 61, No. 2, 1975

PERMUTATION POLYNOMIALS OVER THE RATIONAL NUMBERS

CLIFTON E. CORZATT

Nonlinear polynomials, over the rational numbers, which permute the integers $0, 1, \cdots N$ are investigated. The function $\nu(N)$ represents the minimum degree of all such polynomials. It is shown that

$$\left[\frac{N+1}{4}\right] \leqq \nu(N) \leqq N-1 \quad \text{for all} \quad N \geqq 13 .$$

It is also shown that $\nu(N) \leqq N-2$ for N odd and $N \geqq 7$, that $\nu(N) \leqq N-3$ for $N = 2 \bmod 6$, and that if $\varepsilon > 0$ then $\nu(N) \geqq ((N-1)/2)(1-\varepsilon)$ for N sufficiently large.

1. **Introduction.** We wish to study polynomials with rational coefficients which permute the integers $0, 1, \cdots, N$. Specifically, if we fix N, then are we able to find nonlinear polynomials of this type which have degree less than N? If so, how small can the degree of such a polynomial be? If $N > 4$ we will show that there are polynomials whose degree is less than N. For certain infinite classes of integers we can show that there are polynomials whose degree is less than $N-1$ and $N-2$. Moreover, we show that if $\varepsilon > 0$ then for N sufficiently large the degree of such a polynomial is bounded below by $(N-1)(1-\varepsilon)/2$.

This problem was suggested by Professor L. A. Rubel and arose in the following context. Polya showed that if an entire analytic function of exponential type less than log 2 has integer values at each nonnegative integer, then it is a polynomial. A proof of this theorem is given on page 175 of *Entire Functions* by R. P. Boas. Rubel conjectures that if an entire analytic function of exponential type less than π permutes the nonnegative integers then it is the function $f(z) = z$. He gives the function $f(z) = z + \cos(\pi z)$ as an example of an entire analytic function of exponential type π which permutes the nonnegative integers.

The problem which we study here is an analogue in which we assume $f(z)$ is a polynomial and that it permutes only the integers $0, 1, \cdots, N$. We show that the degree of the polynomial is fairly large with respect to N or it is of degree 1. Rubel's conjecture says that an entire analytic function which permutes the nonnegative integers is of relatively large exponential type (compared to log 2) or it is a polynomial of degree 1. As far as we know this work bears no relationship to the extensive collection of papers which

consider permutation polynomials over finite fields. We note that Professor Charles Wells has compiled a bibliography of these papers.

We begin by defining a somewhat more general class of polynomials. Let $f(k)$ be a function whose domain consists of the integers $0, 1, \cdots, N$ and whose range is contained in the integers. We denote the class of all such functions as $\mathscr{F}(N)$. Given $f(k)$ in $\mathscr{F}(N)$ we define the polynomial

$$\begin{aligned}\tilde{f}(x) &= f(0) + x(-f(0) + f(1)) + \cdots \\ &+ \frac{x(x-1)\cdots(x-j+1)}{j!} \sum_{k=0}^{j} (-1)^{j-k} f(k) \binom{j}{k} + \cdots \\ &+ \frac{x(x-1)\cdots(x-N+1)}{N!} \sum_{k=0}^{j} (-1)^{N-k} f(k) \binom{N}{k} .\end{aligned} \tag{1}$$

This polynomial is the Newton Interpolation Polynomial associated with the points $(k, f(x))$ for $k = 0, 1, \cdots, N$ [3, 44]. Thus, $\tilde{f}(x)$ has the property that $\tilde{f}(k) = f(k)$ for $k = 0, 1, \cdots, N$.

We are interested in functions in $\mathscr{F}(N)$ which are permutations. In other words, functions which map the integers $0, 1, \cdots, N$ onto themselves. Let $\pi(k)$ denote a permutation on $0, 1, \cdots, N$ and let $\mathscr{S}(N)$ denote the class of all such permutations. There are $(N+1)!$ such permutations in $\mathscr{S}(N)$. The polynomial $\tilde{\pi}(x)$ which is associated with $\pi(k)$ in $\mathscr{S}(N)$ by (1) is called the permutation polynomial associated with $\pi(k)$.

From (1) it follows that if $\pi(k)$ is in $\mathscr{S}(N)$ then the degree of $\tilde{\pi}(x)$ is at most N. The permutations $\pi(k) = k$ and $\pi(k) = N - k$ yield the linear permutation polynomials $\tilde{\pi}(x) = x$ and $\tilde{\pi}(x) = N - x$, respectively. In order to study the questions posed above we define

$$\nu(N) = \min_{\pi(k) \in \mathscr{S}(N)} \{\text{degree of } \tilde{\pi}(x) \mid \tilde{\pi}(x) \neq x \text{ and } \tilde{\pi}(x) \neq N - x\} . \tag{2}$$

In other words, if we consider all permutations on $0, 1, \cdots, N$ then $\nu(N)$ will be the minimal degree of all the associated permutation polynomials, except for x and $N - x$. In §2 we discuss the problem of finding upper bounds for $\nu(N)$, and in §3 we obtain a lower bound for $\nu(N)$.

2. **Upper bounds for $\nu(N)$.** When N is 2, 3, or 4 the value of $\nu(N)$ can easily be computed by hand. For N equal to 5, 6, 7, or 8 we have evaluated $\nu(N)$ on a computer by considering all permutations on $0, 1, \cdots, N$. For N equal to 9, 10, 11 or 12 we have considered a large number of permutations and can establish non-trivial upper bounds for $\nu(N)$. The following table summarizes what we can conclude about $\nu(N)$ by direct computation.

TABLE 1

$\nu(2) = 2$	$\nu(5) = 4$	$\nu(8) = 5$	$\nu(11) \leqq 9$
$\nu(3) = 3$	$\nu(6) = 4$	$\nu(9) \leqq 7$	$\nu(12) \leqq 9$
$\nu(4) = 3$	$\nu(7) = 5$	$\nu(10) \leqq 8$	

The above table has inspired the following unanswered questions. Does $N - \nu(N)$ become arbitrarily large for large values of N? Does there exist an increasing sequence of positive integers $\{a_n\}$ such that the sequence $\{a_n - \nu(a_n)\}$ get arbitrarily large for large n?

We can prove the following comparitively weak results. In Theorem 1 we show that if N is even and $N \geqq 4$ then $\nu(N) \leqq N - 1$. In Theorems 2 and 3 we show that if N is odd and $N \geqq 7$ then $\nu(N) \leqq N - 2$. Theorems 1, 2, and 3 together with the fact that $\nu(5) = 4$ give $\nu(N) \leqq N - 1$ for $N \geqq 4$. In Theorem 4 we show that if $N \equiv 2 \bmod 6$ and $N \geqq 8$ then $\nu(N) \leqq N - 3$. We conjecture that if $N \geqq 7$ then $\nu(N) \leqq N - 2$ and in a certain sense Theorems 2, 3, and 4 give two-thirds of this conjecture. We now proceed with the proofs of Theorems 1, 2, 3, and 4.

THEOREM 1. *If N is an even integer and $N \geqq 4$ then $\nu(N) \leqq N - 1$.*

Proof. We define $\pi_0(k)$ in $\mathscr{S}(N)$ to be the permutation which maps 0 to N, N to 0, and leaves everything else fixed. To show $\nu(N) \leqq N - 1$ it suffices to show that the degree of $\tilde{\pi}_0(x)$ is at most $N - 1$. From (1) it is clear that the coefficient of x^N in $\tilde{\pi}_0(x)$ is zero if and only if

$$\sum_{k=0}^{N} (-1)^{N-k} \pi_0(k) \binom{N}{k} = 0 .$$

We have

$$\begin{aligned}
\sum_{k=0}^{N} (-1)^{N-k} \pi_0(k) \binom{N}{k} &= (-1)^N N + \sum_{k=1}^{N-1} (-1)^{N-k} k \binom{N}{k} \\
&\qquad \text{(by the definition of } \pi_0(k)\text{)} \\
&= \sum_{k=1}^{N} (-1)^{N-k} k \binom{N}{k} \text{ (since } N \text{ is even)} \\
&= N \sum_{k=1}^{N} (-1)^{N-k} \binom{N-1}{k-1} \\
&= N \sum_{k=0}^{N-1} (-1)^{N-k+1} \binom{N-1}{k} \\
&= N(1-1)^{N-1}(-1)^{N+1} = 0 .
\end{aligned}$$

In Theorem 2 we show that if $N \geqq 9$ and $N \equiv 1 \bmod 4$ then there is a certain permutation $\pi_1(k)$ in $\mathscr{S}(N)$ such that the degree of $\tilde{\pi}(x)$ is at most $N-2$, and thus $\nu(N) \leqq N-2$. Before we prove Theorem 2 we will prove some easy technical lemmas and define $\pi_1(k)$.

LEMMA 1. *Let N be a positive integer and suppose $f(k)$ is in $\mathscr{F}(N)$. If r is a nonnegative integer and $r < N$ then*

$$\sum_{k=0}^{N}(-1)^k f(k)\binom{N-j}{k} = 0 \text{ for } j = 0, 1, \cdots, r$$

if and only if

$$\sum_{k=0}^{N}(-1)^k f(k)\binom{N-r}{k-s} = 0 \text{ for } s = 0, 1, \cdots, r .$$

Proof. First we assume that

$$\sum_{k=0}^{N}(-1)^k f\binom{N-j}{k} = 0 \text{ for } j = 0, 1, \cdots, r .$$

For $0 \leqq s \leqq r$ we have

$$\begin{aligned}\sum_{j=0}^{r}(-1)^j\binom{s}{j}\sum_{k=0}^{N}(-1)^k f(k)\binom{N-r+s-j}{k} &= \sum_{k=0}^{N}(-1)^k f(k)\sum_{j=0}^{r}(-1)^j\binom{s}{j}\binom{N-r+s-j}{k} \\ &= \sum_{k=0}^{N}(-1)^k f(k)\binom{N-r}{k-s}\end{aligned}$$

(by a well-known combinatorial identity [4, 252]). Thus

$$\sum_{k=0}^{N}(-1)^k f(k)\binom{N-r}{k-s} = 0 \text{ for } s = 0, 1, \cdots, r .$$

Now assume that

$$\sum_{k=0}^{N}(-1)^k f(k)\binom{N-r}{k-s} = 0 \text{ for } s = 0, 1, \cdots, r .$$

For $0 \leqq j \leqq r$ we have

$$\begin{aligned}\sum_{s=0}^{r-j}\binom{r-j}{s}\sum_{k=0}^{N}(-1)^k f(k)\binom{N-r}{k-s} &= \sum_{k=0}^{N}(-1)^k f(k)\sum_{s=0}^{r-j}\binom{r-j}{s}\binom{N-r}{k-s} \\ &= \sum_{k=0}^{N}(-1)^k f(k)\binom{N-j}{k}\end{aligned}$$

(by another well-known combinatorial identity [4, 12]). Thus

$$\sum_{k=0}^{N}(-1)^k f(k)\binom{N-j}{k} = 0 \text{ for } j = 0, 1, \cdots, r .$$

LEMMA 2. *If n and k are nonnegative integers with $n \geqq 1$ and $k + 1 \leqq n$, then* $(n-k)\binom{n}{k} = (k+1)\binom{n}{k+1}$.

Proof. Using the fact that $\binom{n}{k} = (n!/(n-k)!k!)$ we get

$$\begin{aligned}(n-k)\binom{n}{k} &= (n-k)\frac{n!}{(n-k)!k!} \\ &= (k+1)\frac{n!}{(n-(k+1))!\,(k+1)!} \\ &= (k+1)\binom{n}{k+1} .\end{aligned}$$

LEMMA 3. *If N is an even positive integer and $f(k)$ is in $\mathscr{F}(N)$, then*

$$\begin{aligned}\sum_{k=0}^{N}(-1)^k f(k)\binom{N}{k} = \sum_{k=0}^{N/2-1}(-1)^k(f(k) + f(N-k))\binom{N}{k} \\ + (-1)^{N/2} f\left(\frac{N}{2}\right)\binom{N}{N/2} .\end{aligned}$$

Proof. This follows from the facts that $(-1)^k = (-1)^{N-k}$ when N is even and $\binom{N}{k} = \binom{N}{N-k}$.

LEMMA 4. *If N is an even positive integer then*

$$2\sum_{k=0}^{N/2-1}(-1)^k\binom{N}{k} + (-1)^{N/2}\binom{N}{N/2} = 0 .$$

Proof. We use the fact that $\sum_{k=0}^{N}(-1)^k\binom{N}{k} = (1-1)^N = 0$, and apply Lemma 3 with $f(k) = 1$ for $k = 0, 1, \cdots, N$.

LEMMA 5. *If N is an integer which is greater than 2, then*

$$\frac{N}{2}\left(\binom{N}{0} - \binom{N}{1}\right) + \binom{N}{2} = 0 .$$

Proof. We have that

$$\frac{N}{2}\left(\binom{N}{0} - \binom{N}{1}\right) + \binom{N}{2} = \frac{N}{2}(1 - N) + \frac{N(N-1)}{2} = 0 .$$

We now define the permutation $\pi_1(k)$.

DEFINITION 1. If $N \equiv 1 \bmod 4$ and r is the positive integer such that $N = 4r + 1$, then $\pi_1(k)$ is defined by:

(i) $\pi_1(0) = 0$.

(ii) If k is odd and $1 \leqq k \leqq 2r - 1$, then $\pi_1(k) = (k + 1)/2$.

(iii) If k is even and $2 \leqq k \leqq 2r$, then $\pi_1(k) = (N + 1 - k)/2$.

(iv) If k is odd and $2r + 1 \leqq k \leqq N - 4$, then

$$\pi_1(k) = \frac{2N + 1 - k}{2} .$$

(v) If k is even and $2r + 2 \leqq k \leqq N - 3$, then

$$\pi_1(k) = \frac{N + 1 + k}{2} .$$

(vi) $\pi_1(N - 2) = 2r + 1$, $\pi_1(N - 1) = 2r + 2$, and $\pi_1(N) = N$.

For example, if $N = 17$, then $r = 4$ and $\pi_1(k)$ is given in Table 2.

TABLE 2

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\pi_1(k)$	0	1	8	2	7	3	6	4	5	13	14	12	15	11	16	9	10	17

It must be shown that $\pi_1(k)$ is in fact a permutation.

LEMMA 6. *If $N \equiv 1 \bmod 4$ then the function $\pi_1(k)$ of Definition 1 is a permutation.*

Proof. It suffices to show that $\pi_1(k)$ is a function which maps the integers $0, 1, \cdots, N$ onto themselves. It is clear from Definition 1 that 0, $2r + 1$, $2r + 2$ and N are in the image of $\pi_1(k)$. The following four statements also follow from Definition 1.

(i) If $1 \leqq k \leqq r$, then $1 \leqq 2k - 1 \leqq 2r - 1$ and $\pi_1(2k - 1) = k$.

(ii) If $r + 1 \leqq k \leqq 24$, then $2 \leqq N + 1 - 2k \leqq 2r$ and $\pi_1(N + 1 - 2k) = k$.

(iii) If $2r + 3 \leqq k \leqq 3r + 1$, then $2r + 1 \leqq 2N + 1 - 2k \leqq 4r - 3$ and $\pi_1(2N + 1 - 2k) = k$.

(iv) If $3r + 2 \leqq k \leqq 4r$, then $2r + 2 \leqq 2k - (1 + n) \leqq 4r - 2$ and $\pi_1(2k - (1 + N)) = k$.

So $\pi_1(k)$ is an onto function and thus a permutation.

THEOREM 2. *If* $N \geqq 9$ *and* $N \equiv 1 \bmod 4$, *then* $\nu(N) \leqq N - 2$.

Proof. It suffices to show that $\sum_{k=0}^{N-1}(-1)^k\pi_1(k)\binom{N-1}{k} = 0$ and $\sum_{k=1}^{N}(-1)^k\pi_1(k)\binom{N-1}{k-1} = 0$ since this together with Lemma 1 and (1) imply that the degree of $\tilde{\pi}_1(x)$ is at most $N-2$ and thus $\nu(N) \leqq N-2$.

We begin by showing that the first sum is zero. If we let $N = 4r+1$, apply Lemma 3, break the sum into even and odd terms, and evaluate $\pi_1(k)$ by Definition 1 we get that

$$\sum_{k=0}^{N-1}(-1)^k\pi_1(k)\binom{N-1}{k} = \left[(2r+2)\binom{4r}{0} + \sum_{k=1}^{r-1}(6r+2-2k)\binom{4r}{2k}\right] - \left[(2r+2)\binom{4r}{1} + \sum_{k=1}^{r-1}(2r+3+2k)\binom{4r}{2k+1}\right] + (r+1)\binom{4r}{2r}.$$

We now add $(r+1)\sum_{k=0}^{2r-1}2(-1)^k\binom{4r}{k}$ to the sum and subtract $(2r+2)(-1)^k\binom{4r}{k}$ from each term for which $k = 0, 1, \cdots, 2r-1$ to get

$$\sum_{k=0}^{N-1}(-1)^k\pi_1(k)\binom{N-1}{k} = (r+1)\left[\sum_{k=0}^{2r-1}2(-1)^k\binom{4r}{k} + \binom{4r}{2r}\right] + \sum_{k=1}^{r-1}\left[(4r-2k)\binom{4r}{2k} - (2k+1)\binom{4r}{2k+1}\right].$$

The first expression is zero by Lemma 4 and the second expression is zero by Lemma 2.

Now we must show that $\sum_{k=0}^{N-1}(-1)^k\pi_1(k)\binom{N-1}{k} = 0$. Again we let $N = 4r+1$, apply Lemma 3, break the sum into even and odd terms, and evaluate $\pi_1(k)$ to get that

$$\sum_{k=0}^{N-1}(-1)^k\pi_1(k)\binom{N-1}{k} = (4r+2)\left(\binom{4r}{1} - \binom{4r}{0}\right) + (6r+1)\binom{4r}{3} - (2r+3)\binom{4r}{2} + \left[\sum_{k=3}^{r}(6r+3-2k)\binom{4r}{2k-1} - (2r+2k)\binom{4r}{2k-2}\right] - (3r+1)\binom{4r}{2r}.$$

This time we add $-(3r+1)\left(\sum_{k=0}^{2r-1}(2)(-1)^k\binom{4r}{k}\right)$ to the sum, subtract $-(6r+2)(-1)^k\binom{4r}{k}$ from each term for which $k = 0, 1, \cdots,$

$2r-1$, and split the term involving $\binom{4r}{2}$ to get;

$$\sum_{k=0}^{N-1}(-1)^k\pi_1(k) = -(3r+1)\left[\sum_{k=0}^{2r-1}2(-1)^k\binom{4r}{k} - \binom{4r}{2r}\right] + \left[2r\left(\binom{4r}{0} - \binom{4r}{1}\right) + \binom{4r}{2}\right] + \sum_{r}^{k=2}\left[(4r+2k+2)\binom{4r}{2k-2} - (2k-1)\binom{4r}{2k-1}\right].$$

The first part of the right side is zero by Lemma 4, the second by Lemma 5, and the third by Lemma 2. Thus the proof of Theorem 2 is complete.

We now wish to get a similar result for $N \equiv 3 \bmod 4$. We begin by defining a function $\pi_3(k)$ in $\mathscr{F}(N)$ where $N \equiv 3 \bmod 4$.

DEFINITION 2. If N is a positive integer and $N \equiv 3 \bmod 4$ and r is a nonnegative integer such that $N = 4r+3$, then $\pi_3(k)$ is defined by the following conditions.

(i) If k is even and $0 \leqq k \leqq 2r$ then $\pi_3(k) = k/2$.

(ii) If k is odd and $1 \leqq k \leqq 2r+1$ then $\pi_3(k) = (N-k)/2$.

(iii) If k is even and $2r+2 \leqq k \leqq N-1$ then $\pi_3(k) = N-(k/2)$.

(iv) If k is odd and $2r+3 \leqq k \leqq N$ then $\pi_3(k) = (N+k)/2$.

For example, if $N = 15$ then $\pi_3(k)$ is given in Table 3.

TABLE 3

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi_3(k)$	0	7	1	6	2	5	3	4	11	12	10	13	9	14	8	15

We must show that $\pi_3(k)$ is a permutation.

LEMMA 7. *If $N = 4r+3$ where r in nonnegative, then the function $\pi_3(k)$ of Definition 2 is a permutation.*

Proof. It suffices to show that $\pi_3(k)$ maps $0, 1, \cdots, N$ onto itself. The following four statements, which follow from Definition 2 show that $\pi_3(k)$ is onto.

(i) If $0 \leqq k \leqq r$ then $0 \leqq 2k \leqq 2r+1$ and $\pi_3(2k) = k$.

(ii) If $r+1 \leqq k \leqq 2r+1$ then $1 \leqq N-2k \leqq 2r+1$ and $\pi_3(N-2k) = k$.

(iii) If $2r+2 \leqq k \leqq 3r+2$ then $2r+2 \leqq 2N-2k \leqq 4r+2$ and $\pi_3(2N-2k) = k$.

(iv) If $3r+3 \leqq k \leqq 4r+3$ then $2r+3 \leqq 2k-N \leqq 4r+3$ and

$\pi_3(2k - N) = k$.
Thus $\pi_3(k)$ is a permutation.

THEOREM 3. *If* $N \geqq 7$ *and* $N \equiv 3 \bmod 4$ *then* $\nu(N) \leqq N - 2$.

Proof. It will suffice to show that $\sum_{k=0}^{N-1}(-1)^k\pi_3(k)\binom{N-1}{k} = 0$ and that $\sum_{k=1}^{N}(-1)^k\pi_3(k)\binom{N-1}{k-1} = 0$ by Lemma 1 and (1). We begin by showing that the first sum is zero. We let $N = 4r + 3$, apply Lemma 3, evaluate $\pi_3(k)$ by Definition 2, and separate the even and odd terms to get

$$\sum_{k=0}^{N-1}(-1)^k\pi_3(k)\binom{N-1}{k} = (2r+2)\binom{4r+2}{0} + \left[\sum_{k=1}^{r}(2r+2+2k)\binom{4r+2}{2k} - (6r+5-2k)\binom{4r+2}{2k-1}\right] - (r+1)\binom{4r+2}{2r+1}.$$

If we add $(r+1)(\sum_{k=0}^{2r}2(-1)^k\binom{4r+2}{k}$ to the right side of the equation and subtract $(2r+2)(-1)^k\binom{4r+2}{k}$ from each term for $k = 0, 1, \cdots, 2r$, we get

$$\sum_{k=0}^{N-1}(-1)^k\pi_3(k)\binom{N-1}{k} = (r+1)\left[\sum_{k=0}^{2r}2(-1)^k\binom{4r+2}{k} - \binom{4r+2}{2r+1}\right] + \left[\sum_{k=1}^{r}(2k)\binom{4r+2}{2k} - ((4r+2) - (2k-1))\binom{4r+2}{2k-1}\right].$$

The first term is zero by Lemma 4 and the second is zero by Lemma 2. Thus $\sum_{k=0}^{N-1}(-1)^k\pi_3(k)\binom{N-1}{k} = 0$.

We still have $N = 4r + 3$ and now show that

$$\sum_{k=1}^{N}(-1)^k\pi_3(k)\binom{N-1}{k-1} = 0.$$

We make a change of index, letting k run from 0 to $N - 1$, apply Lemma 3, separate the even and odd terms, and evaluate $\pi_3(k)$ by Definition 2 to get

$$\sum_{k=1}^{N}(-1)^k\pi_3(k)\binom{N-1}{k-1}=-(6r+4)\binom{4r+2}{0}+(3r+2)\binom{4r+2}{2r+1}$$
$$+\left[\sum_{k=1}^{r}(2k+2r+1)\binom{4r+2}{2k-1}-(6r+4-2k)\binom{4r+2}{2k}\right].$$

We now add $-(3r+2)\left(\sum_{k=0}^{2r}2(-1)^k\binom{4r+2}{k}\right)$ to the right side and subtract $-(6r+4)(-1)^k\binom{4r+2}{k}$ from each term for $k=0, 1, \cdots, 2r$, to get

$$\sum_{k=1}^{N}(-1)^k\pi_3(k)\binom{N-1}{k-1}$$
$$=-(3r+2)\left[\sum_{k=0}^{2r}2(-1)^k\binom{4r+2}{k}-\binom{4r+2}{2r+1}\right]$$
$$+\left[\sum_{k=1}^{r}-(4r+2-(2k+1))\binom{4r+2}{2k-1}+2k\binom{4r+2}{2k}\right].$$

The first expression is zero by Lemma 4 and the second is zero by Lemma 2. Hence $\sum_{k=1}^{N}(-1)^k\pi_3(k)\binom{N-1}{k-1}=0$ and the proof of Theorem 3 is complete.

COROLLARY 1. *If $N\geqq 4$ then $\nu(N)\leqq N-1$.*

Proof. This follows immediately from Theorems 1, 2, and 3 together with the fact that $\nu(5)=4$ from Table 1.

COROLLARY 2. *If $N\geqq 7$ and N is odd then $\nu(N)\leqq N-2$.*

Proof. This follows from Theorems 2 and 3.

We now turn our attention to the set of positive integers which are congruent to 2 modulo 8. We will show that $\nu(N)\leqq N-3$ for these numbers, and we note that 3 is the largest value of $N-\nu(N)$ which we have found. Again, we begin by defining a function on $0, 1, \cdots, N$ where $N\equiv 2 \bmod 6$ and $N\geqq 8$.

DEFINITION 3. If $N\geqq 8$ and $N\equiv 2 \bmod 6$ we define $\pi_2(k)$ in $\mathscr{T}(N)$ by the following 4 statements.

(i) If $k=0$ then $\pi_2(k)=0$ and if $k=N$ then $\pi_2(k)=N$.
(ii) If $k\equiv 1 \bmod 6$ or $k\equiv 4 \bmod 6$, then $\pi_2(k)=k$.
(iii) If $k\equiv 2 \bmod 6$ and $k\neq N$ or $k\equiv 3 \bmod 6$, then $\pi_2(k)=k+3$.
(iv) If $k\equiv 5 \bmod 6$ or $k\equiv 6 \bmod 6$ and $k\neq 0$, then $\pi_2(k)=k-3$.

For example, if $N=14$ then $\pi_2(k)$ is given in Table 4.

TABLE 4

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi_2(k)$	0	1	5	6	4	2	3	7	11	12	10	8	9	13	14

As with $\pi_1(k)$ and $\pi_3(k)$ we must show $\pi_2(k)$ is a permutation.

LEMMA 8. *The function $\pi_2(k)$ of Definition 3 is permutation.*

Proof. It suffices to show that $\pi_2(k)$ maps $0, 1, \cdots, N$ onto themselves. It is clear from Definition 3 that 0 and N are in the range of $\pi_2(k)$. The following statements also follow from Definition 3 and give that $\pi_2(k)$ is onto.

(i) If $k \equiv 1$ or $4 \bmod 6$ and $1 < k < N$, then $\pi_2(k) = k$.

(ii) If $k \equiv 2$ or $3 \bmod 6$ and $1 < k < N$, then $1 < k + 3 < N$ and $\pi_2(k + 3) = k$.

(iii) If $k \equiv 5$ or $6 \bmod 6$ and $1 < k < N$, then $1 < k - 3 < N$ and $\pi_2(k - 3) = k$.

Thus $\pi_2(k)$ is a permutation.

Before we prove Theorem 4 we give two more lemmas.

LEMMA 9. *If $N \equiv 0 \bmod 6$ then the following three identities hold:*

(i) $\binom{N}{0} + \binom{N}{3} + \binom{N}{6} + \cdots + \binom{N}{N} = (1/3)(2^n + 2)$.

(ii) $\binom{N}{1} + \binom{N}{4} + \binom{N}{7} + \cdots + \binom{N}{N-2} = (1/3)(2^n - 1)$.

(iii) $\binom{N}{2} + \binom{N}{5} + \binom{N}{8} + \cdots + \binom{N}{N-1} = (1/3)(2^n - 1)$.

Proof. These follow immediately from a well-known combinatorial identity. See, for example, Netto [4, 248].

LEMMA 10. *If N and i are non-negative integers then*

$$\sum_{k=i}^{N+i} (-1)^k k \binom{N}{k-i} = 0 .$$

Proof. By a change of index we have that

$$\sum_{k=i}^{N+i} (-1)^k k \binom{N}{k-i} = \sum_{k=0}^{N} (-1)^{k+i}(k+i)\binom{N}{k}$$

$$= i(-1)^i \sum_{k=0}^{N} (-1)^k \binom{N}{k} + (-1)^i \sum_{k=0}^{N} (-1)^k k \binom{N}{k}$$

$$= i(-1)^i(1-1)^N + (-1)^i \sum_{k=1}^{N} (-1)^k N \binom{N-1}{k-1}$$

$$= (-1)^i N \sum_{k=1}^{N-1} (-1)^{k+1} \binom{N-1}{k}$$

$$= (-1)^{i+1} N (1-1)^{N-1} = 0 .$$

THEOREM 4. *If* $N \equiv 2 \bmod 6$ *and* $N \geqq 8$ *then* $\nu(N) \leqq N-3$.

Proof. It suffices to show that $\sum_{k=0}^{N-2} (-1)^k \pi_2(k) \binom{N-2}{k}$, $\sum_{k=1}^{N-1} (-1)^k \pi_2(k) \binom{N-2}{k-1}$, and $\sum_{k=2}^{N} \pi_2(k) \binom{N-2}{k-2}$ are all zero; the result then follows from Lemma 1 and (1) which give us that the degree of $\tilde{\pi}_2(x)$ is at most $N-3$.

We proceed to show that the first sum is zero. We let $N = 6r+2$ and apply Lemma 10 so

$$\sum_{k=0}^{N-2} (-1)^k \pi_2(k) \binom{N-2}{k} = \sum_{k=0}^{6r} (-1)^k (\pi_2(k) - k) \binom{6r}{k} .$$

Now we break the sum into three parts according to congruence classes mod 3 of k, and apply Definition 3 which yields

$$\sum_{k=0}^{N-2} (-1)^k \pi_2(k) \binom{N-2}{k} = -3 \sum_{k=0}^{2r} \binom{6r}{3k} + 0 + 3 \sum_{k=0}^{2r-1} \binom{6r}{3k+2} .$$

It follows by Lemma 9 that the expression on the right is zero. Now we turn to the second sum. Since $N = 6r+2$, it follows from Lemma 10 that

$$\sum_{k=1}^{N-1} (-1)^k \pi_2(k) \binom{N-2}{k-1} = \sum_{k=1}^{6r+1} (-1)^k (\pi_2(k) - k) \binom{6r}{k-1} .$$

Again, breaking the sum up according to residue classes mod 3 and applying Definition 3 we get

$$\sum_{k=1}^{N-1} (-1)^k \pi_2(k) \binom{N-2}{k-1} = 0 + 3 \sum_{k=0}^{2r-1} \binom{6r}{3k+1} - 3 \sum_{k=1}^{2r} \binom{6r}{3k-1} .$$

This expression is equal to zero by Lemma 9.

Finally, we again apply Lemma 10 to get

$$\sum_{k=2}^{N} (-1)^k \pi_2(k) \binom{N-2}{k-2} = \sum_{k=2}^{6r+2} (-1)^k (\pi_2(k) - k) \binom{6r}{k-2} .$$

Using the above decomposition of the sum and by applying Definition 3 we have that

$$\sum_{k=2}^{N}(-1)^k\pi_2(k)\binom{N-2}{k-2} = \left(3\sum_{k=0}^{2r}\binom{6r}{3k} - 1\right) + 0 + \left(-3\sum_{k=1}^{2r}\binom{6r}{3k-2}\right).$$

This expression is equal to zero by Lemma 9, and the proof of Theorem 4 is complete.

We now state a corollary which says that $\nu(N) \leqq N-2$, "two-thirds of the time".

COROLLARY 3. *If* $N \geqq 7$ *and* $N \equiv 1, 2, 3,$ *or* $6 \bmod 6$ *then* $\nu(N) \leqq N-2$.

Proof. This is an immediate consequence of Theorems 2, 3 and 4.

3. Lower Bounds for $\nu(N)$.

We proved in Section 2 that if $\pi(k)$ is a permutation on $0, 1, \cdots, N$, then $\nu(N) < N$ for $N \geqq 4$. In this section we will show that $\nu(N)$ cannot become too small if N is sufficiently large. In fact, we show that for large values of N that the value of $\nu(N)$ cannot be appreciably smaller than $N/2$. Again we concern ourselves with functions in $\mathscr{F}(N)$; i.e. the integer valued functions whose domain consists of $0, 1, \cdots, N$. If $f(k)$ is in $\mathscr{F}(N)$ we are able to associate it with a polynomial, $\tilde{f}(x)$, by (1).

If i is a positive integer and $i < N$, then it follows from (1) that the degree of $\tilde{f}(x)$ is at most $N-i$ if and only if

$$(3) \qquad \sum_{k=0}^{N-j}(-1)^k f(k)\binom{N-j}{k} = 0 \quad \text{for} \quad j = 0, 1, \cdots, i-1.$$

DEFINITION 4. We define M to be a $(N+1)$ by (i) matrix, whose entry in row r and column s is $(-1)^{r-1}\binom{N-s+1}{r-1}$. (In Definition 4 and throughout this chapter we adopt usual convention that $\binom{N}{k} = 0$ whenever $k > N$ or $k < 0$.)

For example, if $N = 4$ and $i = 3$ the matrix M is

$$\begin{pmatrix} \binom{4}{0} & \binom{3}{0} & \binom{2}{0} \\ -\binom{4}{1} & -\binom{3}{1} & -\binom{2}{1} \\ \binom{4}{2} & \binom{3}{2} & \binom{2}{2} \\ -\binom{4}{3} & -\binom{3}{3} & 0 \\ \binom{4}{4} & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ -4 & -3 & -2 \\ 6 & 3 & 1 \\ -4 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

We wish to consider M as a linear transformation which sends $(N+1)$-dimensional row vectors with integer coordinates into i-dimensional row vectors with integer coordinates. The linear transformation is determined by multiplying the $(N+1)$-dimensional vectors on the right by M. We denote by Ker M the set of all $(N+1)$-dimensional vectors with integer coordinates whose image is the i-dimensional zero vector under this linear transformation. We determine a relationship between Ker M and the functions in $\mathscr{F}(N)$.

LEMMA 11. *The vector* $\bar{v} = (v_0, v_1, \cdots, v_N)$ *is in* Ker M *if and only if the polynomial associated with* $f(k) = v_k$ *for* $k = 0, 1, \cdots, N$ *has degree at most* $N - i$.

Proof. Suppose $\bar{v} = (v_0, v_1, \cdots, v_N)$ is in Ker M; i.e. $\bar{v} \cdot M = 0$; then by the definition of matrix multiplication we get

$$\sum_{k=0}^{N} (-1)^k v_k \binom{N-j}{k} = 0 \quad \text{for} \quad j = 0, 1, \cdots, i-1 .$$

Thus the function $f(k) = v_k$ is associated with a polynomial whose degree is at most $N - i$ by (3).

Conversely, if $f(k)$ is associated with a polynomial, $\tilde{f}(x)$, of degree at most $N - i$, then the vector $(f(0), f(1), \cdots, f(N))$ is in ker M by (3).

Thus if we wish to find functions in $\mathscr{F}(N)$ associated with polynomials of degree at most $N - i$ it would be useful to characterize Ker M. Specifically we shall find a basis for Ker M.

DEFINITION 5. If j is an integer and $0 \leqq j \leqq N - i$, then $\bar{v}_j$ is defined to be the $(N+1)$-dimensional row vector

$$\left(\binom{0}{j}, \binom{1}{j}, \binom{2}{j}, \cdots, \binom{N}{j}\right) .$$

For example, $\bar{v}_2 = \left(0, 0, \binom{2}{2}, \binom{3}{2}, \cdots, \binom{N}{2}\right)$.

LEMMA 12. *The vectors* $\bar{v}_0, \bar{v}_1, \cdots, \bar{v}_{N-i}$, *taken over the integers, are a basis for* Ker M.

Proof. We must show that $\bar{v}_0, \bar{v}_1, \cdots, \bar{v}_{N-i}$ are in Ker M, that each vector in Ker M can be written in the form $\sum_{j=0}^{N-i} a_j \bar{v}_j$ where the a_j are integers, and that the vectors $\bar{v}_j$ are linearly independent.

First we show that $\bar{v}_j$ is in Ker M for $j=0, 1, \cdots, N-i$. i.e. $v_jM=0$. For a fixed j this amounts to showing

$$\sum_{k=0}^{N}(-1)^k\binom{k}{j}\binom{N-s}{k}=0 \quad \text{for} \quad s=0, 1, \cdots, i-1 .$$

This follows from a well-known combinatorial identity since $N-s>j$. For example, see Netto [4, 255].

Next we show that each vector in Ker M can be written in the form $\sum_{j=0}^{N-i} a_j\bar{v}_j$ where a_j is an integer. Suppose $\bar{w}=(w_0, w_1, \cdots, w_N)$ is in Ker M. Since $\bar{v}_j$ has zeros in the first j coordinates and a 1 in the $(j+1)^{st}$ coordinate it is possible to find integers $a_0, a_1, \cdots, a_{N-i}$ such that $\bar{u}=\sum_{j=0}^{N-i} a_j\bar{v}_j$ agrees with $\bar{w}$ on the first $N-i+1$ coordinates. The function $f(j)=w_j$ for $j=0, 1, \cdots, N$ is associated with a polynomial $\tilde{f}(x)$ whose degree is at most $N-i$. Thus $\tilde{f}(x)$ is completely determined by $N-i+1$ of its values. In particular $\tilde{f}(x)$ is determined by $\tilde{f}(j)=w_j$ for $j=0, 1, \cdots, N-i$. In other words, if a vector is in Ker M it is completely determined by its first $N-i+1$ coordinates. Since $\bar{u}$ is in Ker M and agrees with $\bar{w}$ on the first $N-i+1$ coordinates, we can conclude that $\bar{u}=\bar{w}$ and $\bar{w}=\sum_{j=0}^{N-i} a_j\bar{v}_j$.

Finally we must show that the vectors $\bar{v}_j$ are linearly independent. If $\sum_{j=0}^{N-i} a_j\bar{v}_j=0$ then we must show that $a_0=a_1=\cdots=a_{N-i}=0$. This is clearly true since $\bar{v}_j$ has zeros in the first j coordinates and a one in the $(j+1)^{st}$ coordinate. Thus the proof of Lemma 12 is complete.

LEMMA 13. *Let p be an odd prime number. If $f(k)$ is in $\mathscr{F}(N)$ and $N\geqq p$ and $\tilde{f}(x)$ has degree at most $p-1$, then p divides $f(p+r)-f(r)$ for $0\leqq r\leqq N-p$.*

Proof. Since the polynomial $\tilde{f}(x+r)$ has degree at most $p-1$ and passes through the points $(0, f(r))$, $(1, f(r+1))$, $\cdots$, $(p, f(p+r))$ we can conclude from (3) that

$$\sum_{k=0}^{p}(-)^k f(r+k)\binom{p}{k}=0 \quad \text{for} \quad 0\leqq r\leqq N-p .$$

Thus p divides $\sum_{k=0}^{p}(-1)^k f(r+k)\binom{p}{k}$ and since p divided $\binom{p}{k}$ for $k=1, 2, \cdots, p-1$ we have that p divides $\sum_{k=1}^{p-1}(-1)^k f(r+k)\binom{p}{k}$, so p divides $f(r)\binom{p}{0}+(-1)^p f(r+p)\binom{p}{p}$. In other words, p divides $f(p+r)-f(r)$.

We now come to the main lemma of this section. Lemma 14

together with some well-known results on primes in an interval will allow us to get lower bounds for $\nu(N)$.

LEMMA 14. *Suppose p is a prime number which is at least 7 and N is an integer such that $2p-1 \leqq N \leqq 4p-5$. If $\pi(k)$ is in $\mathscr{S}(N)$ and the degree of $\tilde{\pi}(x)$ is at most $p-1$, then $\tilde{\pi}(x) = x$ or $\tilde{\pi}(x) = N - x$.*

Proof. If $\tilde{\pi}(x)$ is of degree at most $p-1$, then by Lemma 12 there are integers a_j such that $\sum_{j=0}^{p-1} a_j \bar{v}_j = (\pi(0), \pi(1), \cdots, \pi(N))$ where the $\bar{v}_j$ are the vectors of Definition 5. In other words,

$$\begin{aligned}
\pi(0) &= a_0\binom{0}{0} \\
\pi(1) &= a_0\binom{1}{0} + a_1\binom{1}{1} \\
&\vdots \\
\pi(p-1) &= a_0\binom{p-1}{0} + a_1\binom{p-1}{0} + \cdots + a_{p-1}\binom{p-1}{p-1} \\
\pi(p) &= a_0\binom{p}{0} + a_1\binom{p}{1} + \cdots + a_{p-1}\binom{p}{p-1} \\
&\vdots \\
\pi(N) &= a_0\binom{N}{0} + a_1\binom{N}{1} + \cdots + a_{p-1}\binom{N}{p-1}.
\end{aligned}$$

If r is an integer such that $0 \leqq r \leqq N-p$ then $\pi(p+r) - \pi(r) \equiv 0 \bmod p$ by Lemma 13, and since $\pi(k)$ is a permutation, $\pi(p+r) - \pi(r) = \delta_r p$ where $1 \leqq |\delta_r| \leqq 3$ because $N \leqq 4p-5$. This gives a collection of $N-p+1$ equations of the form

$$\begin{aligned}
&\left(\binom{p+r}{1} - \binom{r}{1}\right)a_1 + \left(\binom{p+r}{2} - \binom{r}{2}\right)a_2 + \cdots \\
&\qquad + \left(\binom{p+r}{p-1} - \binom{r}{p+1}\right)a_{p-1} = \delta_r p\,.
\end{aligned} \tag{4}$$

We focus our attention on certain subsets of $p-1$ of these equations. For example, if $0 \leqq r \leqq N-2p+2$ then $\pi(p+r+j) - \pi(r+j) = \delta_{r+j}p$ where $0 \leqq j \leqq p-2$ gives a subset of $p-1$ equations. If $0 \leqq r \leqq N-2p+2$ then we have the system shown on the following page (equation (5)). If we consider $a_1, a_2, \cdots, a_{p-1}$ as variables and $\delta_r, \delta_{r+1}, \cdots, \delta_{r+p-2}$ as arbitrary constants then (5) consists of $p-1$ linear equations in $p-1$ variables. For the sake of brevity we write the equations in (5) as

$$\begin{aligned} E(r) &= \delta_r p \\ E(r+1) &= \delta_{r+1} p \\ &\vdots \qquad\quad \vdots \\ E(r+p-2) &= \delta_{r+p+2} p \end{aligned}$$

We now consider the following equivalent system:

$$\begin{aligned} E(r) &= \delta_r p \\ E(r+1) - E(r) &= (\delta_{r+1} - \delta_r)p \\ E(r+2) - 2E(r+1) + E(r) &= (\delta_{r+2} - 2\delta_{r+1} + \delta_r)p \\ &\vdots \qquad\qquad\qquad \vdots \\ \sum_{j=0}^{p-2} (-1)^i \binom{p-2}{j} E(r+p-2-j) &= p \sum_{j=0}^{p-2} (-1)^j \binom{p-2}{j} \delta_{r+p-2-j} \,. \end{aligned}$$

In other words, we replace the equation $E(r+i) = \delta_{r+i} p$ with the i^{th} finite difference of the first $i+1$ equations.

We now wish to compute the new coefficients of the a_k for $1 \leqq k \leqq p-1$. If $0 \leqq i \leqq p-2$ then the coefficient of a_k in the equation

$$(5) \quad \begin{cases} \left(\binom{p+r}{1} - \binom{r}{1}\right)a_1 + \left(\binom{p+r}{2} - \binom{r}{2}\right)a_2 + \cdots + \left(\binom{p+r}{p-1} - \binom{r}{p-1}\right)a_{p-1} = \delta_r p \\ \left(\binom{p+r+1}{1} - \binom{r+1}{1}\right)a_1 + \left(\binom{p+r+1}{2} - \binom{r+1}{2}\right)a_2 + \cdots + \left(\binom{p+r+1}{p-1} - \binom{r+1}{p-1}\right)a_{p-1} = \delta_{r+1} p \\ \qquad\qquad \vdots \qquad\qquad\qquad\qquad\qquad \vdots \\ \left(\binom{2p+r-2}{1} - \binom{p+r-2}{2}\right)a_1 + \left(\binom{2p+r-2}{2} - \binom{p+r-2}{2}\right)a_2 + \cdots + \left(\binom{2p+r-2}{p-1} - \binom{p+r-2}{p-1}\right)a_{p-1} = \delta_{r+p-2} p \\ \sum_{j=0}^{i} (-1)^j \binom{i}{j} E(r+i-j) = p \sum_{j=0}^{i} (-1)^j \binom{i}{j} \delta_{r+i-j} \end{cases}$$

is

$$\sum_{j=0}^{i} (-1)^j \binom{i}{j} \left\{ \binom{p+r+i-j}{k} - \binom{r+i-j}{k} \right\}$$

and this sum is equal to

$$\binom{p+r}{k-i} - \binom{r}{k-i}$$

by a well-known combinatorial identity [4, 252]. We note that $\binom{p+r}{k-i} - \binom{r}{k-i} = 0$ when $i \geqq k$ so an explicit representation of the new system is at the bottom of the page. This system's matrix of coefficients is an upper triangular matrix whose diagonal entries are $\binom{p+r}{1} - \binom{r}{1} = p$. The determinant of the matrix is p^{p-1} so the system is non-singular and therefore with fixed δ's there is an unique solution. We now wish to show that either all the δ's equal 1 or else they all equal -1.

If we assume that $0 \leqq r \leqq N - 2p + 1$, the last equation in the system (6) is

$$pa_{p-1} = p\sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}\delta_{r+p-1-j} .$$

and since $r \leqq N - 2p + 1$ we can replace r with $r + 1$ and get the equation

$$pa_{p-1} = p\sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}\delta_{r+p-2-j}$$

Thus

$$\begin{aligned}(7)\qquad &\sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}\delta_{r+p-1-j} - \sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}\delta_{r+p-2-j} \\ &= \sum_{j=0}^{p-1}(-1)^j\binom{p-1}{j}\delta_{r+p-1-j} = 0 .\end{aligned}$$

$$\left\{\begin{aligned}&\left(\binom{p+r}{1}-\binom{r}{1}\right)a_1+\left(\binom{p+r}{2}-\binom{r}{2}\right)a_2+\cdots \\ &\qquad+\left(\binom{p+r}{p-1}-\binom{r}{p-1}\right)a_{p-1}=p\delta_r \\ &\left(\binom{p+r}{1}-\binom{r}{1}\right)a_2+\cdots \\ &\qquad+\left(\binom{p+r}{p-2}-\binom{r}{p-2}\right)a_{p-1}=p(\delta_{r+1}-\delta_r) \\ &\qquad\vdots\qquad\qquad\vdots \\ &\left(\binom{p+r}{1}-\binom{r}{1}\right)a_{p-1} = p\sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}\delta_{r+p-2-j}\end{aligned}\right.$$

It is easy to see that $(-1)^j\binom{p-1}{j} \equiv 1 \bmod p$ so we get $\sum_{j=0}^{p-1} \delta_{r+p-1-j} \equiv 0 \bmod p$ and in particular if $r = 0$ we get

$$\sum_{j=0}^{p-1} \delta_j \equiv 0 \bmod p . \tag{8}$$

If we assume that $0 \leqq r \leqq N - 2p$ we can replace r with $r + 1$ in (7) so

$$\sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} \delta_{r+p-1-j} - \sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} \delta_{r+p-j} = 0$$

and

$$\sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} \delta_{r+p-j} - \sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} \delta_{r+p-1-j}$$
$$= \sum_{j=0}^{p} (-1)^j \binom{p}{j} \delta_{r+p-j} = 0 .$$

Thus $\sum_{j=0}^{p} (-1)^j \binom{p}{j} \delta_{r+p-j} \equiv 0 \bmod p$ and since $\binom{p}{j} \equiv 0 \bmod p$ for $1 \leqq j \leqq p - 1$ we get $\delta_r \equiv \delta_{r+p} \bmod p$ for $0 \leqq r \leqq N - 2p$. Because we have assumed that $N \leqq 4p - 5$ and $p \geqq 7$ we have that $1 \leqq |\delta_\lambda| \leqq 3$ and since $\delta_r \equiv \delta_{r+p} \bmod p$ we conclude that

$$\delta_r = \delta_{r+p} \quad \text{for} \quad 0 \leqq r \leqq N - 2p . \tag{9}$$

We now consider two cases. First we suppose that $2p - 1 \leqq N < 3p - 1$ which implies that $|\delta_\lambda| \leqq 2$ for $0 \leqq r \leqq N - p$. If there exists an r such that $\delta_r = 2$ and $0 \leqq r \leqq p - 1$ then

$$\pi(r + p) = 2p + \pi(r) . \tag{10}$$

Let t be the integer between 0 and N with the property $\pi(t) = \pi(r) + p$. We claim that $t \neq r + 2p$. If $r + 2p > N$ this is clear, and if $r + 2p \leqq N$ then $\pi(r + 2p) - \pi(r + p) = \delta_{r+p}p = \delta_r p = 2p$ by (9) and (10). We add this equation to (10) and get,

$$\pi(r + 2p) - \pi(r) = 4p$$

which is impossible so $t \neq r + 2p$, and since $\pi(t) \neq \pi(r)$ and $\pi(t) \neq \pi(r + p)$ we have that $t \neq r$ and $t \neq r + p$. We conclude that $t \not\equiv r \bmod p$. If $t + p \leqq N$ let $u = t + p$, and otherwise let $w = t - p$. From Lemma 13 and the fact that $\pi(t) = \pi(r) + p$ we get

$$\pi(r) \equiv \pi(r + p) \equiv \pi(t) \equiv \pi(u) \bmod p$$

and r, $r + p$, t, and u are distinct. This is not possible for $N < 3p - 1$.

Similarly, if $2p-1 \leqq N < 3p-1$ and $0 \leqq r \leqq p-1$ then $\delta_r \neq -2$. So if $0 \leqq r \leqq p-1$ then $|\delta_r| = \pm 1$. From (8) we get

$$\delta_0 = \delta_1 = \cdots = \delta_{p-1} = 1$$

or

$$\delta_0 = \delta_1 = \cdots = \delta_{p-1} = -1 ,$$

and from (9) we conclude that

$$\delta_0 = \delta_1 = \cdots = \delta_{N-p} = 1$$

or

$$\delta_0 = \delta_1 = \cdots = \delta_{N-p} = -1 .$$

In the second case we assume that $3p-1 \leqq N < 4p-4$ and that $|\delta_r| > 1$ for some r such that $0 \leqq r \leqq p-1$. So

$$\pi(r+p) - \pi(r) = \delta_r p ,$$

and by (9)

$$\pi(r+2p) - \pi(r+p) = \delta_{r+p} p = \delta_r p .$$

By adding the equations we get

$$\pi(r+2p) - \pi(r) = 2\delta_r p .$$

Since we are assuming $|\delta_r| > 1$ we get $|\pi(r+2p) - \pi(r)| \geqq 4p$. This is impossible because $N < 4p-4$. We conclude that $|\delta_r| = 1$ for $0 \leqq r \leqq p-1$.

By applying (8) and (9) as we did above, we obtain

$$\delta_0 = \delta_1 = \cdots = \delta_{N-p} = 1$$

or

$$\delta_0 = \delta_1 = \cdots = \delta_{N-p} = -1 .$$

Now we are able to complete the proof of Lemma 14. First we assume that $\delta_0 = \delta_1 = \cdots = \delta_{N-p} = 1$. We have shown that the system (5) has a unique solution for fixed δ's. If $a_1 = 1$ and $a_2 = a_3 = \cdots = a_{p-1} = 0$ we have a solution, and consequently the only solution. We conclude that

$$(\pi(0), \pi(1), \cdots, \pi(N)) = a_0 \vec{v} + \vec{v}_1$$

and since $\pi(k)$ is in $\mathscr{S}(N)$ it follows that $a_0 = 0$. Therefore $(\pi(0), \pi(1), \cdots, \pi(N)) = (0, 1, \cdots, N)$ and $\tilde{\pi}(x) = x$.

Next we assume that $\delta_0 = \delta_1 = \cdots = \delta_{N-p} = -1$. In this case

we get the unique solution if $a_1 = -1$ and $a_2 = a_3 = \cdots = a_{p-1} = 0$. Thus

$$(\pi(0), \pi(1), \cdots, \pi(N)) = a_0\bar{v}_0 - \bar{v}$$

and $\pi(k)$ is in $\mathscr{S}(N)$ if and only if $a_0 = N$. Therefore $(\pi(0), \pi(1), \cdots, \pi(N)) = (N, N-1, \cdots, 0)$ and $\tilde{\pi}(x) = N - x$. The proof of Lemma 14 is now complete.

We now apply Lemma 14 and the theorem commonly known as Bertrand's postulate to get an absolute lower bound for $\nu(N)$ when $N \geqq 13$. Bertrand's postulate states that if N is an integer greater than 3, then there is a prime number p such that $N < p < 2N - 2$ [2, 373].

THEOREM 5. *We have the inequality*

$$\nu(N) \geqq \frac{N+1}{4} \quad \textit{for} \quad N \geqq 13 .$$

Proof. We claim that if $N \geqq 13$ then there is a prime number p such that $2p - 1 \leqq N \leqq 4p - 5$. This is shown by way of contradiction. If N is the smallest integer without this property then $N = 4p - 4$ for some prime p. By Bertrand's Postulate we conclude there is a prime q such that $p < q < 2p - 2$, so $2q - 1 < 4p - 5 < N$ and $4q - 5 > 4p - 5$. Since $N = 4p - 4$ we get the $4q - 5 \geqq N$ and thus $2q - 1 \leqq N \leqq 4q - 5$. This contradicts the condition placed on N.

If $\pi(k)$ is in $\mathscr{S}(N)$ with $N \geqq 13$, p is a prime such that $2p - 1 \leqq N \leqq 4p - 5$, and the degree of $\tilde{\pi}(x)$ is at most $p - 1$, then by Lemma 14 it follows that $\tilde{\pi}(x) = x$ or $\tilde{\pi}(x) = N - x$. We therefore conclude that $\nu(N) \geqq p - 1$ and $p - 1 \geqq (N-1)/4$, so Theorem 5 is proved.

Next we apply Lemma 14 along with the following consequence of The Prime Number Theorem.

LEMMA 15. *If $0 < \varepsilon < 1$, then there is a number $K(\varepsilon)$ such that for every $N > K(\varepsilon)$ there is a prime number between N and $(1 + \varepsilon)N$.*

Proof. A proof is given in Hardy and Wright [2, 371].

We now show that if N is sufficiently large then $\nu(N)$ is bounded below by a number which is just a bit smaller than $(N-1)/2$.

THEOREM 6. *Given ε, such that $0 < \varepsilon < 1$, if N is sufficiently*

large then $\nu(N) \geqq ((N-1)/2)(1-\varepsilon)$.

Proof. We choose $K(\varepsilon)$ as in Lemma 15. We claim that for $N > 4K(\varepsilon)$ there exists a prime number p such that $2p - 1 \leqq N \leqq (2(1+\varepsilon)p) - 1$. We prove the claim by way of contradiction. Let $N_1 > 4K(\varepsilon)$ be the smallest integer which does not satisfy the claim. It follows that there is a prime p_1 such that $N_1 = [2(1+\varepsilon)p_1]$ for this is the first integer greater than $(2(1+\varepsilon)p_1) - 1$. Since $4p_1 > N$ we have $p_1 > N_1/4 > K(\varepsilon)$, so by Lemma 15 there is a prime q such that $p_1 < q < (1+\varepsilon)p_1$. This implies that $2q - 1 < 2(1+\varepsilon)p_1 - 1$ and since $N_1 = [2(1+\varepsilon)p_1]$ we have $2(1+\varepsilon)p_1 - 1 < N_1$ so $2q - 1 < N_1$. Moreover, since $2(1+\varepsilon)(q-p_1) > 1$ we have $2q(1+\varepsilon) - 1 \geqq 2p_1(1+\varepsilon)$ and $2p_1(1+\varepsilon) \geqq N_1$ so $2q(1+\varepsilon) - 1 \geqq N_1$. We now have $2q - 1 \leqq N_1 \leqq 2q(1+\varepsilon) - 1$ where q is prime and this contradicts our assumption for N_1.

If $N > 4K(\varepsilon)$ and $\pi(k)$ is in $\mathscr{S}(N)$ there is a prime p such that $2p - 1 \leqq N \leqq 2(1+\varepsilon)p - 1$. Thus if the degree of $\tilde{\pi}(x)$ is at most $p - 1$ then by Lemma 14 we have that $\tilde{\pi}(x) = x$ or $\tilde{\pi}(x) = N - x$. But,

$$\frac{N+1}{2(1+\varepsilon)} - 1 \leqq p - 1$$

so

$$\begin{aligned} \nu(N) &\geqq \frac{N+1}{2(1+\varepsilon)} - 1 \\ &\geqq \frac{N-1}{2}(1-\varepsilon) . \end{aligned}$$

References

1. R. P. Boas, *Entire Functions*, Academic Press, Inc., 1954.
2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, 1938.
3. F. B. Hildebrand, *Introduction to Numerical Analysis*, McGraw-Hill Book Co., Inc., 1956.
4. E. Netto, *Lehrbuch der Combinatorik*, Verlag Von B. G. Teubner, 1901.

Received December 20, 1974.

St Olaf College