MATH. SCAND. 1 (1953)

PERMUTATION IN RECURSIVE ARITHMETIC

R. L. GOODSTEIN

The recursive definition of the sum of two natural numbers [4] is asymmetrical so that in recursive arithmetic the commutative property of addition is a *theorem* and not a characteristic of the definition as it is for instance in the theory of aggregates. A simple inductive proof of the identity $a+b = b+a$, based on a recursive definition of addition, was first given by Dedekind [1]. The method of proof readily extends to cover sums of any *specified* number of terms, as for instance in the identities

$$(a+b)+c = (a+c)+b \tag{0.1}$$

$$\big((a+b)+c\big)+d = \big((a+d)+c\big)+b. \tag{0.2}$$

The method is however inadequate for the general problem of which (0.1) and (0.2) are particular instances, the problem of showing that the sum of a *variable* number of numbers is independent of the order in which the numbers are taken. To establish this result, which is the object of the present note, we must construct recursive definitions of the familiar processes of *transposition* and *permutation.*

Given a recursive function $a(k)$ we define $\tau(k, n)$ by the recursive equations

$$\tau(k, 0) = a(k), \qquad \tau(k, n+1) = \tau(k, n)+a(n+k+1) ;$$

a simple induction shows that $\tau(k, n)$ satisfies the relation

$$\tau(p, q)+\tau(p+q+1, r) = \tau(p, q+r+1) \tag{1.0}$$

for any non-negative integers p, q, r.

Denoting the recursive function $1\dot{-}(1\dot{-}x)$ as usual by $\operatorname{sg} x$, we define for all p, q

$$\sigma(p, q) = \operatorname{sg}\big((q+1\dot{-}p)\,\tau(p, q\dot{-}p)\big)$$

so that for all p, q, n

$$\sigma(p, p+n) = \tau(p, n) \tag{1.1}$$

Received July 30, 1953.

$$(1.2) \qquad \sigma(q+n+1, q) = 0 \;;$$

in particular $\sigma(1, n+1) = \tau(1, n)$.

It follows that if $q \geqq p$

$$(1.3) \qquad \sigma(p, q+1) = \sigma(p, q)+a(q+1)\,.$$

If $r \leqq s \leqq t$ then

$$(1.4) \qquad \sigma(r, s)+\sigma(s+1, t) = \sigma(r, t) \;;$$

if $t = s$ the result follows by (1.2), and if $t = s+k+1$, $k \geqq 0$, writing $s = r+p$, $p \geqq 0$, we have

$$\begin{aligned}\sigma(r, s)+\sigma(s+1, t) &= \sigma(r, r+p)+\sigma(s+1, s+k+1)\\ &= \tau(r, p)+\tau(r+p+1, k)\\ &= \tau(r, p+k+1) = \sigma(r, t)\end{aligned}$$

which completes the proof of (1.4).

We prove next that, for $1 \leqq r \leqq n$,

$$(1.5) \qquad \sigma(1, n) = \sigma(1, r\dot{-}1)+a(r)+\sigma(r+1, n)$$

and for $1 \leqq r < r+s \leqq n$

$$(1.6) \qquad \sigma(1, n)$$
$$= \sigma(1, r\dot{-}1)+a(r)+\sigma\big(r+1, (r+s)\dot{-}1\big)+a(r+s)+\sigma(r+s+1, n)\,.$$

By (1.2) we see that (1.5) holds when $n = 1$ (and so $r = 1$); if (1.5) holds for $n = k$, and if $1 \leqq r \leqq k+1$, then for $r = k+1$

$$\sigma(1, r\dot{-}1)+a(r)+\sigma(r+1, k+1) = \sigma(1, k)+a(k+1) = \sigma(1, k+1)$$

by (1.3), and for $1 < r = k$ (so that $k = r = p+2$, $p \geqq 0$)

$$\begin{aligned}\sigma(1, r\dot{-}1)+a(r)+\sigma(r+1, k+1) &= \sigma(1, p+1)+a(p+2)+a(k+1)\\ &= \sigma(1, k)+a(k+1), \qquad \text{by (1.3)},\\ &= \sigma(1, k+1)\end{aligned}$$

and for $1 \leqq r < k$ (so that $k \geqq r+1$)

$$\begin{aligned}\sigma(1, r\dot{-}1)+a(r)+\sigma(r+1, k+1) &= \sigma(1, r\dot{-}1)+a(r)+\sigma(r+1, k)+a(k+1)\\ &= \sigma(1, k)+a(k+1), \qquad \text{by hypothesis},\\ &= \sigma(1, k+1)\,.\end{aligned}$$

Further, the reader verifies easily that (1.5) is also valid in the case $1 = r = k$, $n = 2$. This completes the inductive proof of (1.5).

It follows that

$$\begin{aligned}&\sigma(1, r\dot{-}1)+a(r)+\sigma\big(r+1, (r+s)\dot{-}1\big)+a(r+s)+\sigma(r+s+1, n)\\&\quad=\sigma\big(1, (r+s)\dot{-}1\big)+a(r+s)+\sigma(r+s+1, n)=\sigma(1, n)\end{aligned}$$

which is (1.6).

The next step is to define an interchange of $a(r)$ with $a(r+s)$ leaving the other terms unchanged. Let

$$\theta(r, s, k)=\{k+\big((r+s)\dot{-}k\big)\,\overline{\mathrm{sg}}\,|k\dot{-}r|\}\dot{-}(k\dot{-}r)\,\overline{\mathrm{sg}}\,|(r+s)\dot{-}k|\,;$$

then, if $k \neq r,\ k \neq r+s,\ \overline{\mathrm{sg}}\,|k\dot{-}r|=\overline{\mathrm{sg}}\,|(r+s)\dot{-}k|=0$ and so

$$\theta(r, s, k)=k\ ;$$

if $k=r$,

$$\theta(r, s, k)=r+\big((r+s)\dot{-}r\big)=r+s,$$

and if $k=r+s$,

$$\theta(r, s, k)=(r+s)\dot{-}s=r\,.$$

Hence if $b(r, s, k)=a\big(\theta(r, s, k)\big)$ then

$$\begin{aligned}b(r, s, k)&=a(k) &&\text{if } k\neq r,\ k\neq r+s\,,\\&=a(r+s) &&\text{if } k=r\,,\\&=a(r) &&\text{if } k=r+s\,.\end{aligned}$$

To form the sum of the $a(k)$ with $a(r)$ and $a(r+s)$ transposed we introduce the recursive functions $\tau^\star(r, s, k, n)$ and $\sigma^\star(r, s, p, q)$ by the equations

$$\begin{aligned}\tau^\star(r, s, k, 0)&=b(r, s, k)\\\tau^\star(r, s, k, n+1)&=\tau^\star(r, s, k, n)+b(r, s, n+k+1)\\\sigma^\star(r, s, p, q)&=\mathrm{sg}\,\big((q+1)\dot{-}p\big)\cdot\tau^\star(r, s, p, q\dot{-}p)\,.\end{aligned}$$

We have to prove, for $n \geqq 1$,

$$\tau^\star(r, s, 1, n)=\tau(1, n)\ ; \tag{2.0}$$

to this end we start by establishing, for $0 \leqq k < r$,

$$\sigma^\star(r, s, 1, k)=\sigma(1, k)\,. \tag{2.1}$$

If $r=1$ (so that $k=0$), and if $r>1$ and $k=0$ the truth of (2.1) is obvious. If (2.1) holds for $k=p$ then for $k=p+1<r$

$$\sigma(1, p+1)=\sigma(1, p)+a(p+1)$$

and

$$\begin{aligned}\sigma^\star(r, s, 1, p+1)&=\sigma^\star(r, s, 1, p)+b(r, s, p+1)\,, &&\text{as in (1.3),}\\&=\sigma^\star(r, s, 1, p)+a(p+1)\,, &&\text{since } p+1<r\,,\end{aligned}$$

whence (2.1) holds for any k.

We require also two companion theorems to (2.1): For $r \leqq k < r+s$

$$\sigma^\star(r, s, r+1, k) = \sigma(r+1, k) \tag{2.2}$$

and for $r+s \leqq k$

$$\sigma^\star(r, s, r+s+1, k) = \sigma(r+s+1, k)\ . \tag{2.3}$$

The proofs are similar to that of (2.1). Since

$$\tau(1, n) = \sigma(1, n+1) \qquad \text{and} \qquad \tau^\star(r, s, 1, n) = \sigma^\star(r, s, 1, n+1)\ ,$$

(2.0) now follows from (1.6), the analogous result for the function $\sigma^\star$, and the identity $a+b+c+d+e = a+d+c+b+e$.

Since a permutation may be regarded as the result of repeated transpositions, it remains only to define recursively a sequence of transpositions. Given three recursive functions $r(n)$, $s(n)$, and $a(n)$ we define, for all non-negative integers k,

$$\begin{aligned} B(0, k) &= a(k)\,, \\ B(n+1, k) &= B\big(n, \theta\big(r(n), s(n), k\big)\big)\ . \end{aligned}$$

It has been proved by R. Péter [3, § 5] that equations of this form define a primitive recursive function so that $B(n, k)$ is primitive recursive.

For each n, $B(n+1, k)$ is a transposition of $B(n, k)$ such that

$$\begin{aligned} B(n+1, k) &= B(n, k) && \text{if} \quad k \neq r(n),\ k \neq r(n)+s(n), \\ &= B\big(n, r(n)+s(n)\big) && \text{if} \quad k = r(n), \\ &= B\big(n, r(n)\big) && \text{if} \quad k = r(n)+s(n)\ . \end{aligned}$$

If we define the sum function $T(n, k, p)$ by the equations

$$\begin{aligned} T(n, k, 0) \quad &= B(n, k)\,, \\ T(n, k, p+1) &= T(n, k, p)+B(n, k+p+1)\,, \end{aligned}$$

then taking $B(n, k)$ for $a(k)$ and $B(n+1, k)$ for $b(r, s, k)$, with $r = r(n)$, $s = s(n)$, in the proof of (2.0), we find that, for any n,

$$T(n+1, 1, p) = T(n, 1, p)$$

and so

$$T(n, 1, p) \quad = T(0, 1, p) = \tau(1, p)$$

for all n and p, which shows that the sum $a(1)+a(2)+ \ldots +a(p+1)$ is unchanged by any rearrangement of its terms.

The foregoing theorems and proofs are all formalisable in the equation calculus [2].

BIBLIOGRAPHY

1. R. Dedekind, *Was sind und was sollen die Zahlen*, Braunschweig, 1888.
2. R. L. Goodstein, *Constructive formalism*, Leicester, 1951.
3. R. Péter, *Rekursive Funktionen*, Budapest, 1951.
4. Th. Skolem, *Begründung der elementaren Arithmetik durch die rekurrierende Denkweise ohne Anwendung scheinbarer Veränderlichen mit unendlichem Ausdehnungsbereich*, Skrifter utgit av Vid.-Selsk. i Kristiania, I, 1923 No. 6, 1–38.

UNIVERSITY COLLEGE, LEICESTER, ENGLAND