SUMS OF FOUR OR MORE VALUES OF $\mu x^2 + \nu x$
FOR INTEGERS $x^*$

BY GORDON PALL†

1. Introduction. My object is to prove the following theorem.

THEOREM 1. Let $0 < \nu < \mu$, $f(x) = \mu x^2 + \nu x$. Let $T$ denote the table of all sums of four values of $f(x)$ for integers $x$ arranged in order of magnitude. The largest gap between consecutive entries of $T$ is

$$\mu - \nu, \text{ if } \mu \geq 3\nu/2; \quad 5\nu - 3\mu, \text{ if } \mu \leq 3\nu/2. \tag{1}$$

An immediate corollary is the following result.

THEOREM 2. Let $0 < \nu < \mu$, $s \geq 4$. The largest gap in the table of all sums of $s$ values of $f(x)$ for integers $x$ is

$$\mu - \nu, \text{ if } s\mu \geq (s + 2)\nu; \quad (s + 1)\nu - (s - 1)\mu, \text{ if } s\mu \leq (s + 2)\nu. \tag{2}$$

For, if $s \geq 4$, we need only add $(s - 4)f(-1)$ to every entry of $T$, notice that a gap $\mu - \nu$ actually occurs from $4f(0)$ to $f(-1) + 3f(0)$, that no gap greater than $\mu - \nu$ can exceed $5\nu - 3\mu - (s - 4)(\mu - \nu)$, and that the last number actually occurs, when it is positive, as the gap from $s f(-1)$ to $f(1) + (s - 1)f(0)$.

Let us now recall‡ that the only quadratic functions $q(x)$ which are integers $\geq 0$ for every integer $x$, and which take the values 0 and 1 for certain integers $x$, are obtained from the function

$$\frac{1}{2}mx^2 + \frac{1}{2}(m - 2)x, \tag{3}$$

where $m$ is a positive integer, by replacing $x$ by $x - k$ or $k - x$, $k$ an integer. By Theorem 2, the table of all sums of $s$ values of $q(x)$ possesses as its maximum gap the number 1 if $3 \leq m \leq s + 2$, $m - (s + 1)$ if $m \geq s + 2$. One corollary is that every integer $\geq 0$ is a sum of $m - 2$ values of (3) for integers $x$, all but four of which are 0 or 1, at least if $m \geq 6$; and of four values if $m = 3, 4, 5$; (previously proved by Dickson).

* Presented to the Society, November 29, 1930.
† National Research Fellow in Mathematics, California Institute of Technology.
Our problem, since we allow $x$ to have all integer values, is very much simpler than Dickson's in this Bulletin (vol. 33 (1927), pp. 713–720; vol. 34 (1928), pp. 63–72 and pp. 205–217).

2. Proof of Theorem 1. We require two lemmas.

**Lemma 1.** The equations
\[ a = x_1^2 + \cdots + x_4^2, \quad b = x_1 + \cdots + x_4, \]
are solvable in integers $x_i$ if and only if
\[
\begin{align*}
(4) & \quad a \equiv b \pmod{2}, \quad 4a \geq b^2, \quad 4a - b^2 \text{ not of the form } 4k(8v + 7). \\
(5) & \quad a \equiv b \pmod{2},
\end{align*}
\]

**Lemma 2.** The equation
\[ p = (3x_1^2 + 2x_1) + \cdots + (3x_4^2 + 2x_4) \]
is solvable in integers $x_i$, for every $p \geq 0$.

Let $B_a$ denote the largest $b$, for a given $a \geq 0$, for which equations (4) are solvable in integers $x_i$. If $a \not\equiv 0 \pmod{4}$, $B_a$ is, by Lemma 1, the largest integer $b \equiv a \pmod{2}$ and satisfying (5). Hence
\[
(6) \quad (B_a + 2)^2 > 4a, \quad (a \not\equiv 0 \pmod{4}).
\]
Then all values $b$ for which (4) are solvable are
\[
(7) \quad B_a, \quad B_a - 2, \quad B_a - 4, \ldots, \quad B_a + 2, \quad B_a.
\]

We verify that, if $a$ is odd,
\[
(8) \quad B_{a+1} \leq B_a + 1,
\]
for otherwise $B_{a+1} \geq B_a + 3$, $(B_{a+1} - 1)^2 > 4a$, which contradicts $(B_{a+1})^2 \leq 4(a+1)$.

**Case I.** Then $a \geq 3v$. Then $2v$ and $\mu - v$ are permitted as gaps in $T$. In view of (7) we can pass by differences $2v$ to $a\mu + B_a\nu$ from any element $a\mu + b\nu$ of $T$, if $a$ is odd. In view of (8) we can pass from $a\mu + B_a\nu$ to $(a+1)\mu + B_{a+1}\nu$ by an increment $\leq \mu - v$. Trivially,

*A modification of a lemma of Cauchy, this is evident from the identity $4a - b^2 = (x_1 + x_2 - x_3 - x_4)^2 + (x_1 - x_2 + x_3 - x_4)^2 + (x_1 - x_2 - x_3 + x_4)^2$.

† This is equivalent to the readily demonstrable fact that every integer $\geq 4$ and of the form $3p + 4$ is a sum of four squares prime to 3.
(a + 2)u - B_{a+2}v - \{ (a + 1)u + B_{a+1}v \} \leq u - v.

Hence, by induction from a to a+2, we pass throughout the table.

Case II. \((5/3)v < \mu < 3v\). Then \(\delta = 2\mu - 4v\) and \(-\delta\) are both \(\leq \mu - v\). Hence, if \(a \equiv 1 \pmod{4}\) and \(b - 2 \geq -B_{a+2}\) we can reach \(a\mu + B_{a}v\) from the entry \(a\mu + bv\) by successive increments \(\mu - v\), \(\mu - v\), \(-\delta\), over entries of \(T\). Thus we can pass from \(\mu - v\) to \(\mu + v\), thence over \(2\mu, 3\mu - v, 4\mu - 2v, 5\mu - 3v\) and hence to \(5\mu + 3v\). If \(a \equiv 1 \pmod{4}\) and \(\geq 5\) we pass from \(a\mu + B_{a}v\) to \((a+1)\mu + (B_{a} - 1)v, (a+2)\mu + (B_{a} - 2)v, (a+4)\mu + (B_{a} - 6)v\), and hence to \((a+4)\mu + B_{a+4}v\), completing the induction.

Case III. Finally we have the interesting case \(\mu \leq 5v/3\).

Denote by \(M_\mu\) the class of all \(\mu a + bv\) such that

\[ p = 3a + 2b, \quad 4a \geq b^2, \quad a \equiv b \pmod{2}, \quad (5_3). \]

By Lemmas 1 and 2 there exists a solution \(a, b\) of (9) for every integer \(p \geq 0\). Table \(T\) coincides with the ordered class of all the elements of all classes \(M_\mu\).

Let \(A_\mu, a_\mu\) denote, respectively, the largest and the least values of \(a\) satisfying (9); and \(b_\mu, B_\mu\) the corresponding \(b\)'s. If \(p\) is odd the values \(a\) of \(M_\mu\) are

\[ A_\mu, A_\mu - 4, A_\mu - 8, \ldots, a_\mu; \]

the corresponding \(b\)'s being \(b_\mu, b_\mu + 6, b_\mu + 12, \ldots, B_\mu\). Then also \(b_\mu \leq 1, B_\mu \geq -3, a_\mu \geq 1,\) and

\[ 4(a_\mu + 4) < (b_\mu - 6)^2, \quad 4(a_\mu - 4) < (B_\mu + 6)^2, \quad (p \text{ odd}). \]

If \(p\) is odd the difference between two adjacent elements of \(M_\mu\) is allowable, since

\[ 4\mu - 6v \leq \mu - v, \quad \text{and} \quad 6v - 4\mu \leq 5v - 3\mu. \]

The increment from an element \(a\mu + bv\) of \(M_\mu\) to an element \(a\mu + b_\mu v\) of \(M_{\mu+1}\) is \(\leq \mu - v\) or \(5v - 3\mu\), respectively, if

\[(i) \quad \mu \geq 1.5v, \quad a_\mu \geq a_1 + 1; \quad \text{or} \quad (ii) \quad \mu \leq 1.5v, \quad a_1 \leq a_2 + 3.\]

Hence the theorem for the present case will follow from the following lemma.
LEMMA 3. For every even $p \geq 2$,

\begin{align*}
(11) & \quad A_p \leq A_{p-1} + 1, \quad a_{p+1} \leq a_p + 1; \\
(12) & \quad a_{p-1} \leq a_p + 3, \quad A_p \leq A_{p+1} + 3.
\end{align*}

The proof of (11) is typical. By (9) with $p - 1$ and $p$ in place of $\ell$, $A_p = A_{p-1} + 1$ (mod 4). Hence the contrary of (11) would imply $A_p = A_{p-1} + 5 + 4v_1$, and consequently $b_\ell = b_{\ell-1} - 7 - 6v_1$, where $v_1 \geq 0$. Hence, by $4A_p \geq (b_p)^2$,

$$4(A_{p-1} + 5 + 4v_1) \geq (b_{p-1} - 7 - 6v_1)^2,$$

contradicting (10) with $p - 1$ in place of $p$, since

$$4(1 + 4v_1) \leq 2(1 + 6v_1)(6 - b_{p-1}) + (6v_1 + 1)^2.$$

THE CALIFORNIA INSTITUTE OF TECHNOLOGY

GROUPS GENERATED BY TWO OPERATORS WHOSE SQUARES ARE INVARIANT

BY G. A. MILLER

It is well known that two operators of order two generate the dihedral group whose order is twice the order of the product of these operators. The groups that can be generated by two operators which have a common square are also well known. The groups considered in the present article are obviously a generalization of these two categories of well known groups. We shall represent their two generators by $s$ and $t$. From the fact that $s^2$ and $t^2$ are invariant operators of the group $G$ generated by $s$ and $t$ it results directly that

$$s^{-1}sts = t^{-1}stt = ts = (st)^{-1}s^2t^2,$$

$$s^{-1}tss = t^{-1}tst = st = (ts)^{-1}s^2t^2.$$

From these equations it follows that the abelian group $H$ generated by $s^2$, $t^2$, and $st$ is invariant under $G$ and that its index under $G$ cannot exceed 2.

A necessary and sufficient condition that $H$ be identical with $G$ is that $G$ be abelian and can be generated by the product of two of its operators and the squares of these operators. It is not