JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 77B, Nos. 3 & 4, July–December 1973

Triangles Generated by Powers of Triplets on the Unit Circle

Charles R. Johnson* and Morris Newman

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(June 7, 1973)

Let α, β, γ be three distinct complex numbers of modulus 1. It is shown that there is essentially one exception to the following statement: For some positive integer m, 0 is in the closed convex hull of α^m, β^m, γ^m. The exception occurs for the normalized triple

$$1,\ e^{2\pi i/7},\ e^{2k\pi i/7},$$

where $k=3$ or 5. This question was motivated by the problem of determining when a positive integer m and a nonzero $n\times 1$ vector x exist such that

$$x^*A^mx=0,$$

where A is a given matrix of $M_n(C)$.

Key words: Convex hull; unit circle; Weyl's Theorem.

In connection with determining for what $A\epsilon M_n(C)$ the equation

$$x^*A^mx=0$$

is solvable by some positive integer [1] m and some $n\times 1$ vector $x\neq 0$, the following question arose: How many distinct points $\alpha_1, \ldots, \alpha_l$ on the unit circle are in general required to insure that for some positive integer m, 0 lies in the convex hull of $\{\alpha_1^m, \ldots, \alpha_l^m\}$? We find that in general $l=4$ such points are required. However, our main result is that under appropriate normalization in the case $l=3$ there is exactly one exceptional set.

Throughout α, β, γ will denote three distinct points on the unit circle in the complex-plane. We shall denote the triangular solid generated by their mth powers by

$$T_m(\alpha, \beta, \gamma)=\mathrm{Co}\{\alpha^m, \beta^m, \gamma^m\}.$$

Our goal is to determine for which triples α, β, γ, there is a positive integer m such that

$$0\epsilon T_m(\alpha, \beta, \gamma).$$

For this purpose we shall identify two triples (α, β, γ), and $(\alpha', \beta', \gamma')$ if one may be obtained from the other via any combination of permutation, reflection, and simultaneous rotation. We shall also identify these two triples if

$$\{T_m(\alpha, \beta, \gamma)\,|\,m\epsilon I^+\}=\{T_m(\alpha', \beta', \gamma')\,|\,m\epsilon I^+\}.$$

AMS Subject Classification: 52–00, 15A24, 15–A63.

*The work of the first author was done while he was a National Academy of Sciences-National Research Council Postdoctoral Research Associate at the National Bureau of Standards, Washington, D.C. 20234.

507-714 O - 73 - 5

Subsequent to this identification there is exactly one exception (α, β, γ) to the statement:

There is an $m \epsilon I^+$ *such that* $0 \epsilon T_m(\alpha, \beta, \gamma)$.

With respect to the identification mentioned above, we shall take our triples to be in normalized form:

$$\alpha = e^{2\pi i z_1},\ \beta = e^{2\pi i z_2},\ \gamma = 1$$

where $0 < z_1 < z_2 < 1$. Letting $\{r\}$ denote the fractional part of the real number r, we shall then say that the positive integer m is a solution to the normalized problem (*) if

$$\text{(i)}\ \{mz_{j_1}\} \leqslant 1/2$$

$$\text{(ii)}\ \{mz_{j_2}\} \geqslant 1/2,$$

and

$$\text{(iii)}\ \{mz_{j_2}\} - \{mz_{j_1}\} \leqslant 1/2,$$

where $(j_1, j_2) = (1, 2)$ or $(2, 1)$. It is clear that m is a solution to the normalized problem (*) if and only if $0 \epsilon T_m(\alpha, \beta, \gamma)$.

Example. If $z_1 = \frac{1}{7}$ and $z_2 = \frac{3}{7}$ or $\frac{5}{7}$, then the system (*) is not solvable. Only the values $1 \leqslant m \leqslant 7$ need be considered and it is routine to check that for each of these values at least one of (i), (ii), or (iii) is not satisfied.

Our main result is:

THEOREM: *Let* α, β, γ *be distinct complex numbers such that* $|\alpha| = |\beta| = |\gamma| = 1$. *Then there is a positive integer* m *such that* $0 \epsilon \mathrm{T_m}(\alpha, \beta, \gamma)$ *if and only if the normalized form of* $\{\alpha, \beta, \gamma\}$ *is not* $\{e^{\frac{2\pi i}{7}}, e^{\frac{2k\pi i}{7}}, 1\}$, $k = 3$ *or* 5.

PROOF: It suffices to consider the normalized problem (*). The necessity then follows from the given example. For the sufficiency we distinguish 5 possibilities (1) z_1 and z_2 are irrational and rationally independent; (2) z_1 and z_2 are irrational and rationally dependent; (3) exactly one of z_1 and z_2 is rational; (4) z_1 and z_2 are rational with distinct denominators in reduced form; (5) z_1 and z_2 are rational with the same denominator in reduced form.

For cases 1, 2, and 3 we shall employ a well-known theorem of Weyl:

LEMMA 1 (Weyl [2]): (a) If z is irrational, then the sequence $\{nz\}_{n=1}^{\infty}$ is uniformly distributed on the unit interval. (b) If z_1 and z_2 are rationally independent, then the ordered pairs $(\{nz_1\}, \{nz_2\})$, $n = 1, 2, \ldots$, are uniformly distributed on the unit square.

In case 1, the normalized problem (*) is easily solved because of Lemma 1, part (b). For case 2 we assume without loss of generality that the pair z_1, z_2 is of the form

$$bz,\ az + r$$

where z is irrational, $r = \frac{l_1}{l_2}$ is rational, and a, b, l_1, l_2 are integers with $a, b, l_2 > 0$. If $a = b$, this case may be transformed into case 3 by rotation. Thus we also assume without loss of generality that $a > b$. Suppose $m = m'l_2$, $m' > 0$ and integral, and let

$$c = \{mz\} = \{m'(l_2 z)\}.$$

Then by Lemma 1, part (a), we may obtain c arbitrarily close to any real number between 0 and 1 by choice of m'. Since $a > b > 0$, we may choose ϵ_1, ϵ_2 so that

$$\epsilon_1 > 0,\ \epsilon_2 > 0,\ \epsilon_1 + \epsilon_2 < \frac{1}{2}$$

and

$$\frac{b}{a} = \frac{1 - 2\epsilon_2}{1 + 2\epsilon_1}\cdot$$

Next choose

$$0 < \epsilon < \min\left\{\frac{1}{2a} - \frac{\epsilon_1}{a}, \frac{\epsilon_2}{b}\right\}.$$

Then choose m' so that

$$0 \leq c - \left(\frac{1}{2a} + \frac{\epsilon_1}{a}\right) < \epsilon.$$

We then have

$$\{m(az+r)\} = \{ac\} = ac$$

$$\{m(bz)\} = \{bc\} = bc$$

and

$$\{m(az+r)\} - \{m(bz)\} = ac - bc.$$

Since

$$\frac{1}{2} + \epsilon_1 \leq ac < \frac{1}{2} + \epsilon_1 + \epsilon a$$

and

$$\frac{1}{2} - \epsilon_1 \leq bc < \frac{1}{2} - \epsilon_2 + \epsilon b,$$

it follows that

$$\frac{1}{2} \leq ac \leq 1$$

$$0 \leq bc \leq \frac{1}{2}$$

and

$$0 \leq ac - bc \leq \frac{1}{2}$$

so that (*) is solvable in case 2. In case 3, (*) may be solved using Lemma 1, part (a).

For the remaining cases we assume that in reduced form

$$z_1 = \frac{h}{n_1},\ z_2 = \frac{k}{n_2}\cdot$$

Without loss of generality we may assume that h or k is 1. If either n_i is even, then $0 \epsilon T_{n_{i/2}}(\alpha, \beta, 1)$ and we are finished. Thus we may assume that n_1 and n_2 are odd. Suppose (case 4) that $n_1 \neq n_2$, and $n =$ g.c.d. (n_1, n_2). By the Chinese Remainder Theorem, the congruences

$$2hm \equiv n_1 - n \bmod n_1$$

and

$$2km \equiv n_2 + n \bmod n_2$$

have a solution m, which may be taken positive. It then follows that for such an m, (i), (ii), and (iii) are satisfied which completes the discussion of this case.

Finally we assume (case 5) that $n_1 = n_2 = n$ which is odd. Without loss of generality we take $h=1$ and since z_2 is in reduced form we have g.c.d. $(k, n)=1$.

LEMMA 2: If $n>2$, $1<k<n$ are integers, $z_1 = \frac{1}{n}$, $z_2 = \frac{k}{n}$, and $(k, n)=1$, then the following are equivalent:

(1) the system (*) is solvable for $k = x$;
(2) the system (*) is solvable for $k = x'$, where $xx' \equiv 1 \pmod{n}$; and
(3) the system (*) is solvable for $k \equiv (1-x) \pmod{n}$.

PROOF: The equivalence of (1) and (2) follows from the fact

$$\{T_m(e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i x}{n}}, 1) \,|\, m \in I^+\}$$

$$= \{T_m(e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i x'}{n}}, 1) \,|\, m \in I^+\}.$$

The equivalence of (1) and (3) follows from the fact that

$$\overline{e^{\frac{2\pi i}{n}}(e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i x}{n}}, 1)} = (1, e^{\frac{2\pi i(1-x)}{n}}, e^{\frac{2\pi i}{n}}).$$

Now if k is even, we may choose $m = \frac{n-1}{2}$ to satisfy (*) since $n \neq 1$ is odd. Thus we may assume because of Lemma 2 that k and k' are both odd, where $1 < k' < n$ is the unique solution to $kk' \equiv 1 \bmod n$. Because of Lemma 2, we may also assume that

$$1 < k \leq \frac{p+1}{2}.$$

However since $\left(\frac{p+1}{2}\right)' = 2$ which is even, we need only consider

$$1 < k \leq \frac{p-1}{2}.$$

We now wish to determine for which n (*) is solvable under our present assumptions.

Let $m \equiv k'\left(\frac{n+j}{2}\right) \bmod n$ where j *is odd* and $n < k'j < 2n$. Then since k' is odd, we have $\left\{\frac{m}{n}\right\} = \left\{\frac{1}{2} + \frac{k'j}{2n}\right\} = \left\{1 + \frac{k'j-n}{2n}\right\} = \left\{\frac{k'j-n}{2n}\right\} = \frac{k'j-n}{2n} < \frac{n}{2n} = \frac{1}{2}$ which means that (i) is satisfied.

If $1 < j < n$ also, then $\left\{\frac{mk}{n}\right\} = \left\{\frac{n+j}{2n}\right\} = \left\{\frac{1}{2} + \frac{j}{2n}\right\} = \frac{1}{2} + \frac{j}{2n} > \frac{1}{2}$ so that (ii) is satisfied.

Finally $\left\{\frac{mk}{n}\right\}-\left\{\frac{m}{n}\right\}=\frac{1}{2}+\frac{j}{n}-\frac{k'j-n}{2n}=1-\left(\frac{(k'-1)j}{2n}\right)$ which is less than $\frac{1}{2}$ *if* $(k'-1)j>n$.

We now have 4 requirements on j for (*) to be solvable. Since $k' \neq 1$ is odd they reduce to

$$j \text{ odd}$$

and

$$\frac{n}{k'-1}<j<\frac{2n}{k'}$$

Thus if the interval $\left(\frac{n}{k'-1}, \frac{2n}{k'}\right)$ is of length greater than or equal to 2, there will be a solution with j odd and integral. Thus we require

$$\frac{2n}{k'}-\frac{n}{k'-1}\geqslant 2$$

or

$$\frac{2(k'-1)n-nk'}{k'(k'-1)}\geqslant 2$$

or

$$n \geqslant 2\,\frac{k'(k'-1)}{(k'-2)}\,.$$

As a function of k', $2\,\frac{k'(k'-1)}{(k'-2)}$ is increasing for $k'>2+\sqrt{2}$. If $k'=\frac{n-3}{2}$, our requirement becomes

$$n\geqslant\frac{(n-3)(n-5)}{(n-7)}$$

or

$$n\geqslant 15.$$

It remains to check the cases in which $k'=3$ or $\frac{n-1}{2}$ for general odd n and the cases $n=3$, 5, 7, 9, 11, 13. By straightforward computation, the latter yield that (*) is solvable in all cases except that mentioned in the example. In the former case we have that

$$1-\left(\frac{n-1}{2}\right)'\equiv 3 \bmod n$$

since n is odd. Thus by Lemma 2 it suffices to check $k=3$.

In case $k=3$, it is easily checked that $m=\left[\frac{n}{6}\right]+1$, where $[\cdot]$ denotes the greatest integer function, satisfies (*) for $n\geqslant 12$. The remaining case $n<12$ have already been checked so that the proof is complete.

COROLLARY: *If* $l\geqslant 4$ *and* $\alpha_1, \alpha_2, \ldots, \alpha_l$ *are distinct complex numbers of absolute value* 1, *then there is a positive integer* m *such that*

$$0\in\mathrm{Co}\{\alpha_1^m, \ldots, \alpha_l^m\}.$$

PROOF: Because of the Theorem, it suffices to check the set of four points $e^{\frac{2\pi i}{7}}, e^{\frac{6\pi i}{7}}, e^{\frac{10\pi i}{7}}, 1$. Since 0 is actually in their convex hull, the result is confirmed.

References

[1] Johnson, C.R., Powers of Matrices with Positive Definite Real Part, to appear.

[2] Weyl, H. Über die Gleichverteilung von Zahlen mod Eins, Math. Ann. **77** (1916), pp. 313–352.

(Paper 77B3&4–389)