GENERATING REFLECTIONS FOR $U(2, p^{2n})$

D. W. CROWE

1. **Introduction.** In any finite field, $GF[q^2]$, whose order, $q^2 = p^{2n}$, is an even power of the prime p, there is an involutory automorphism, $x \to x^q$, which defines a *conjugate*, $\bar{x} = x^q$. The unitary group, $U(2, q^2)$, can be represented as the group of all 2×2 matrices of the form

$$\begin{Bmatrix} x & y \\ -\bar{y}D & \bar{x}D \end{Bmatrix},$$

where $x, y, D \in GF[q^2]$ and $x\bar{x} + y\bar{y} = D\bar{D} = 1$ [3, p. 132]. A *unitary reflection* is such a matrix exactly one of whose characteristic roots is unity. It has been shown in [2] that $U(2, 3^2)$ is generated by two unitary reflections of period four. It is the purpose of the present note to show that $U(2, q^2)$ (q odd) is generated by two unitary reflections of period $q+1$. An immediate consequence of this is the existence of a new infinite family of regular unitary polygons, one for each odd q. (In the sequel $q = p^n$ is always odd.)

2. **The generating reflections.** Let λ be a generator of the multiplicative group of $GF[q^2]$, and let $\delta = \lambda^{q-1}$, so that $\delta\bar{\delta} = 1$. We try to find

$$R = \begin{Bmatrix} x & y \\ -\bar{y}\delta & \bar{x}\delta \end{Bmatrix}$$

so that R and

$$S = \begin{Bmatrix} 1 & 0 \\ 0 & \delta \end{Bmatrix}$$

generate $U(2, q^2)$, and are both reflections with characteristic roots $1, \delta$. In particular, $x + \bar{x}\delta = 1 + \delta$. One choice of x satisfying this equation is $x = (1+\delta)/2$. Then $y = (1-\delta)/2$ satisfies $x\bar{x} + y\bar{y} = 1$. For these values of x and y the powers of R can be verified by induction to be

$$R^k = \begin{Bmatrix} x_k & y_k \\ y_k & x_k \end{Bmatrix},$$

where $x_k = (1+\delta^k)/2$ and $y_k = (1-\delta^k)/2$. We now write $t = (q+1)/2$ and $R^t = T$, from which, since $\delta^t = -1$, we have

$$T = \begin{Bmatrix} 0 & 1 \\ 1 & 0 \end{Bmatrix}.$$

Presented to the Society, August 29, 1961; received by the editors March 28, 1961.

Finally we let

$$P = TST = \begin{Bmatrix} \delta & 0 \\ 0 & 1 \end{Bmatrix}.$$

We proceed to verify that the group $\mathcal{G} = \{R, S\}$ generated by R and S has order $|\mathcal{G}| > (q^2-1)q(q+1)/2$. That is, the order of the subgroup $\mathcal{G}$ of $U(2, q^2)$ is greater than half the known order [**3**, p. 132] of $U(2, q^2)$, so that $\mathcal{G} \cong U(2, q^2)$. It is sufficient to verify that matrices in $\mathcal{G}$ have more than $(q^2-1)q/2$ distinct first rows, since left multiplication by the powers of S yields $q+1$ different matrices for each first row. In fact, the matrices $R^kP^iS^j$ $(k=1, \cdots, t-1; i, j=1, \cdots, q+1)$ have exactly $(q-1)(q+1)^2/2$ different first rows, for $(q-1)/2$ first rows (x_k, y_k) appear among the powers of R, and each of these has its first and second components multiplied independently by the $q+1$ powers of δ. (It is necessary to note that in the range $k, m=1, \cdots, t-1$ no x_k is a multiple by δ^r of x_m unless $k=m$. For let $x_k = \delta^r x_m$. Multiplying each side by its conjugate and simplifying yields $\delta^k + \bar{\delta}^k = \delta^m + \bar{\delta}^m$. On putting $\delta^{-1} = \bar{\delta}$ this becomes $(\delta^{k+m}-1)(\delta^k - \delta^m) = 0$. But $\delta^{k+m} \neq 1$ in the range considered. Thus $k=m$. The same holds for the second components.) But $(q-1)(q+1)^2/2 > (q^2-1)q/2$, as required. This proves the

THEOREM. *The unitary reflections*

$$R = \frac{1}{2}\begin{Bmatrix} 1+\delta & 1-\delta \\ 1-\delta & 1+\delta \end{Bmatrix} \quad \textit{and} \quad S = \begin{Bmatrix} 1 & 0 \\ 0 & \delta \end{Bmatrix} \textit{ generate } U(2, q^2).$$

3. **Regular unitary polygons over** $GF[q^2]$. The notion of regular complex polygon introduced by Shephard [**4**] has an obvious analog in the unitary plane, $UG(2, q^2)$, over $GF[q^2]$. A *regular unitary polygon* in $UG(2, q^2)$ is a configuration of points and lines ("vertices" and "edges") whose group of automorphisms is generated by two unitary reflections, one, R, permuting cyclically the vertices on one edge, and the other, S, permuting cyclically the edges at one of these vertices [**1**, p. 79]. Now take R and S as in the Theorem. The images of the line $x+y=1$ and the point $(1, 0)$ on it, under the group $\{R, S\}$, constitute the edges and vertices of such a polygon. Its vertices, being the $(q^2-1)q$ first rows of matrices in $\{R, S\}$, are in fact exactly the points of the unit circle $x\bar{x}+y\bar{y}=1$. It has the same number of edges, since there are $q+1$ edges at each vertex and $q+1$ vertices on each edge. For example, in the case $q=3$ the polygon has $(3^2-1)3=24$ vertices lying by fours on 24 edges, with four edges at each vertex. Its group, $U(2, 3^2)$, is of order $(3^2-1)3(3+1)=96$. It is an isomorphic

copy of Shephard's 4(96)4 [2; 4]. All other values of $q=p^n$ yield new polygons.

References

1. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups*, Berlin-Göttingen-Heidelberg, 1957.
2. D. W. Crowe, *Regular polygons over* $GF[3^2]$, Amer. Math. Monthly **68** (1961), 762–765.
3. L. E. Dickson, *Linear groups*, Teubner, Leipzig, 1901.
4. G. C. Shephard, *Regular complex polytopes*, Proc. London Math. Soc. (3) **2** (1952), 82–97.

University College, Ibadan, Nigeria