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, $x \rightarrow x^q$, which defines a conjugate, $\tilde{x} = x^q$. The unitary group, $U(2, q^2)$, can be represented as the group of all $2 \times 2$ 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 $U(2, 3^3)$ 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 $\lambda$ be a generator of the multiplicative group of $GF[q^2]$, and let $\delta = \lambda \ell_{-1}$, so that $\delta \delta = 1$. 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

$$
T = \begin{bmatrix}
    0 & 1 \\
    1 & 0
\end{bmatrix}.
$$
Finally we let

\[ P = TST = \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}. \]

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 \( R^k P^i S^j \) \( (k = 1, \ldots, t - 1; i, j = 1, \ldots, q + 1) \) 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 \( \delta \). (It is necessary to note that in the range \( k, m = 1, \ldots, t - 1 \) no \( x_k \) is a multiple by \( \delta \) of \( x_m \) unless \( k = m \). For let \( x_k = \delta x_m \). Multiplying each side by its conjugate and simplifying yields \( \delta^k + \overline{\delta}^k = \delta^m + \overline{\delta}^m \). On putting \( \delta^{-1} = \overline{\delta} \) 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

\[ R = \frac{1}{2} \begin{pmatrix} 1 + \delta & 1 - \delta \\ 1 - \delta & 1 + \delta \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} \]

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 \( xx + yy = 1 \). 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


University College, Ibadan, Nigeria