BULL. AUSTRAL. MATH. SOC. MOS 05C20, 20B25

VOL. 6 (1972), 53-59.

An algebraic characterization of finite symmetric tournaments

J.L. Berggren

A tournament T is called symmetric if its automorphism group is transitive on the points and arcs of T. The main result of this paper is that if T is a finite symmetric tournament then T is isomorphic to one of the quadratic residue tournaments formed on the points of a finite field $GF(p^n)$, $p^n \equiv 3\ (4)$, by the following rule: If $a, b \in GF(p^n)$ then there is an arc directed from a to b exactly when $b - a$ is a non-zero quadratic residue in $GF(p^n)$.

Throughout this paper T will denote a finite tournament, $A(T)$ its automorphism group, and the number of points in T will be written as $|T|$. We call T a *symmetric* tournament if $A(T)$ is transitive on the points and arcs of T. If a and b are points of T and if an arc of T is directed from a to b we write $a > b$.

The purpose of this paper is to prove the following theorem.

THEOREM A. *Let T be a symmetric tournament. Then there is a finite field $GF(p^n)$, where $p^n \equiv 3\ (4)$, such that T is isomorphic to the tournament formed on the points of $GF(p^n)$ by the following rule: If $a, b \in GF(p^n)$ then $a > b$ if $b - a = x^2$, for some non-zero $x \in GF(p^n)$. Moreover, identifying T with this tournament, $A(T)$ is the group of all permutations of T of the form $a \to x^2\sigma(a) + c$, where c*

Received 18 August 1971.

ranges over all elements of $GF(p^n)$, x *over all non-zero elements of* $GF(p^n)$, *and* σ *over all field automorphisms of* $GF(p^n)$.

REMARK. Assuming that T is a tournament formed from $GF(p^n)$ in the manner described above, Goldberg [2] proved that the automorphism group of T is as described in the last sentence of Theorem A. However, this result is an immediate corollary of our classification of symmetric tournaments, so we also include it here.

We first state and prove a lemma. The various parts of this lemma are well-known, but we include the statement and proof for completeness.

LEMMA 1. *Let* T *be a symmetric tournament. The following statements are true:*

(i) $A(T)$ *has odd order and (so) is solvable;*

(ii) $A(T)$ *is a primitive permutation group on the points of* T ;

(iii) there is a prime $p \equiv 3 \ (4)$ *and an odd integer* n *such that* $|T| = p^n$.

Proof. Since no element of $A(T)$ can interchange two points of T , $A(T)$ has odd order and is therefore solvable [1]. To prove *(ii)* suppose $B_1, \ldots, B_r$ is a system of imprimitivity for $A(T)$, so $r \geq 2$ and $|B_1| \geq 2$. Let $a, b \in B_1$ and $c \in B_2$. We may assume $a > b$. If $a > c$ then by arc transitivity there exists $\pi \in A(T)$ such that $\pi(a) = a$ and $\pi(b) = c$. Thus $\pi(B_1)$ intersects both B_1 and B_2 non-trivially, which is a contradiction of the definition of a system of imprimitivity. The case $c > a$ also yields a contradiction. Hence $A(T)$ acts primitively on T . Finally, we prove *(iii)*. By *(i)* and *(ii)* we may conclude from Satz 3.2(a) [3, Chapter II] that $|T| = p^n$ for some prime p . For $a \in T$ let $O(a) = \{b \in T \mid a > b\}$. Since $A(T)$ is transitive on the points of T , $|O(a)| = |O(b)|$ for all $a, b \in T$. This implies $|O(a)| = (p^n-1)/2$, so by arc-transitivity $(p^n-1)/2$ divides the order of $A(T)_a$, the stabilizer of a in $A(T)$. Hence $(p^n-1)/2$ is odd and so $p \equiv 3 \ (4)$ and n is odd.

Before proceeding we state some notation. For a prime p and integer $n > 0$ let $V = V(n, p)$ be an n-dimensional vector space over the field of order p and let $V^* = \{a \in V \mid a \neq 0\}$. If $GL(n, p) = GL(V)$ is the group of non-singular linear transformations of V onto V then for each $L \in GL(n, p)$ and $a \in V$ define a permutation $[L, a]$ of V by the following rule: $[L, a](b) = L(b) + a$, for all $b \in V$. In particular, if I denotes the identity of $GL(n, p)$ then $[I, a]$ is simply translation by a. With this notation we now state and prove Theorem 1.

THEOREM 1. *Let T be a symmetric tournament, $|T| = p^n$. Then we may identify the points of T with those of $V(n, p)$ so that*

$$\{[I, a] \mid a \in V\} \leq A(T) \leq \{[L, a] \mid L \in GL(V), a \in V\}.$$

Further, identifying T with V in this manner and setting $O(0) = \{a \in V \mid 0 > a\}$ and $I(0) = \{a \in V \mid a > 0\}$ then the orbits on V^* of $A(T)_0$, the stabilizer of 0 in $A(T)$, are $O(0)$ and $I(0)$. Moreover $O(0) = -I(0)$.

Proof. The first statement is an immediate consequence of our Lemma 1 and of Satz 3.5 [3, Chapter II]. The second statement is immediate, since $A(T)$ is transitive on the arcs of T. To prove the last statement observe that $|O(0)| = (p^n-1)/2$, so $|I(0)| = (p^n-1)/2$. Suppose both a and $-a \in O(0)$. Since $[I, -a] \in A(T)$ we find $-a > 0$ and $0 > -a$, a contradiction. Thus $O(0) = -I(0)$.

REMARK. To fix notation let $A(T)_0 = G$. Then the restrictions of G to $O(0)$ or $I(0)$ yield representations τ_1 and τ_2 respectively of G as a transitive permutation group.

LEMMA 2. *The representations τ_1 and τ_2 are faithful representations of G and are similar.*

Proof. Since both $O(0)$ and $I(0)$ contain half the non-zero elements of V, each contains a basis. Since G consists of *linear* transformations of V it follows that τ_1 and τ_2 are faithful representations of G. The last part of the lemma is proved by considering the map from $O(0)$ onto $I(0)$ given by $a \to -a$, and the map

https://doi.org/10.1017/S0004972700044257 Published online by Cambridge University Press

from $\tau_1(G)$ to $\tau_2(G)$ given by $\tau_1(g) \to \tau_2(g)$. (Again one must recall that the elements of G act linearly on V .)

We next show that G has a cyclic normal subgroup which acts irreducibly on V . We first remark that any finite group A has a maximal normal nilpotent subgroup, called its Fitting subgroup and written $\mathrm{Fit}(A)$.

LEMMA 3. *If* $G = A(T)_0$ *then* $\mathrm{Fit}(G)$ *is cyclic and acts semi-regularly on* V^* .

Proof. As $\mathrm{Fit}(G)$ is nilpotent it is a direct product of its Sylow subgroups, so it suffices to show that if Q is a Sylow subgroup of $\mathrm{Fit}(G)$ then Q is cyclic and acts semiregularly on V^* . Since Q is a characteristic subgroup of $\mathrm{Fit}(G)$ and $\mathrm{Fit}(G) \lhd G$, we conclude $Q \lhd G$. By Lemma 2, G acts faithfully as a transitive group on $O(0)$, so Q is 1/2-transitive on $O(0)$ [4, Proposition 4.4], that is, the orbits of Q on $O(0)$ all have the same length. By the proof of Lemma 2, if U is an orbit of Q on $O(0)$ then $-U$ is an orbit of Q on $I(0)$. Thus viewing Q as a permutation group on V^* , Q is 1/2-transitive on V^* . Now $|Q|$ is odd so, as Q is 1/2-transitive on V^* , it follows from [4, Proposition 9.16] that Q is cyclic and acts semiregularly on V^* .

THEOREM 4. *Let* $H = \mathrm{Fit}(G)$. *Then* H *acts irreducibly on* V .

Proof. We have just shown that H acts semiregularly on V^* , that is, the orbits of H on V^* all have cardinality $|H|$. In particular, since this means $|H| \Big| (p^n - 1)$, $(|H|, p) = 1$. Now suppose H acts reducibly on V . We may apply Maschke's Theorem (as $(|H|, p) = 1$) to conclude $V = U \oplus W$, where U and W are proper H-invariant subspaces of V . Let $|U| = p^m$ and assume without loss of generality that $|U| \leq |W|$. Thus $m \leq [n/2]$, and since n is odd, this means $m \leq (n-1)/2$. Since H acts semiregularly on V^* and U contains an orbit of H on V^* , $|H| < |U| = p^m$. But $H = \mathrm{Fit}(G)$, and since G is solvable it follows from Satz 4.2(b) [3, Chapter III] that $H \geq C_G(H)$, the centralizer in G of H . Thus G/H is isomorphic to a subgroup of $\mathrm{Aut}(H)$, and, as H is cyclic of odd order, $|\mathrm{Aut}(H)| < |H|$. Thus

$|G/H| < |H|$. Hence $|G| = |G/H||H| < p^m p^m \leq p^{n-1}$. But $O(0)$ is an orbit of G and $|O(0)| = (p^n-1)/2$. Hence $(p^n-1)/2 \leq p^{n-1}$. This contradiction shows H acts irreducibly on V , for we may suppose $p^n > 3$.

Now observe that $A(T)$ is represented as a primitive permutation group on V with the following properties:

(1) $N = \{[I, a] \mid a \in V\}$ is an abelian minimal normal subgroup of $A(T)$ acting regularly on V ;

(2) $A(T)_0$ has the abelian normal subgroup $H = \mathrm{Fit}(A(T)_0)$ which acts irreducibly on V .

It is easy to show that, under these hypotheses, N is a minimal normal subgroup of HN . The following theorem is an immediate consequence of these remarks and Satz 3.12 [4, Chapter II].

THEOREM 5. *Let T be a symmetric tournament of order p^n and $A(T)$ the automorphism group of T . Then we may identify the points of T with the points of the Galois field of order p^n , $GF(p^n)$, so that $A(T)$ is a subgroup of $\Gamma(p^n)$, the group of permutations of $GF(p^n)$ of the form $a \to x\sigma(a) + c$, where c runs over the elements of $GF(p^n)$, x runs over $GF(p^n)^*$ (the non-zero elements of $GF(p^n)$), and σ runs over the field automorphisms. Moreover, $A(T)$ contains the subgroup consisting of all translations of $GF(p^n)$, permutations of the form $a \to a + c$, $c \in GF(p^n)$.*

REMARK. The last sentence is easy to show once one observes that $A(T)$ contains an abelian minimal normal subgroup acting regularly on T .

The permutation of $GF(p^n)$ which maps an arbitrary a to $x\sigma(a) + c$ we shall denote by $[x, \sigma, c]$. Further, let $S = \{x^2 \mid x \in GF(p^n)^*\}$ and notice, since $p^n \equiv 3\ (4)$, $S \cup (-S) = GF(p^n)^*$ while $S \cap (-S) = \emptyset$.

THEOREM 6. *Either $O(0) = S$ or $O(0) = -S$.*

https://doi.org/10.1017/S0004972700044257 Published online by Cambridge University Press

Proof. As $|O(0)| = (p^n-1)/2$, if the theorem is false then there are $x, y \in GF(p^n)^*$ such that $0 > x^2$ and $0 > -y^2$. By arc transitivity there is $[\omega, \sigma, 0] = \pi \in A(T)_0$ such that $\pi(x^2) = -y^2$, that is, $\omega = -\left(y\sigma(x^{-1})\right)^2$. Let $u = y\sigma(x^{-1})$. Since $|A(T)_0|$ is odd, $\langle \pi \rangle = \langle \pi^2 \rangle$. Let S be the orbit of 1 under the action of $\langle \pi^2 \rangle$. Now $\pi^0(1) = 1$ and $\pi^2(1) = \omega\sigma(\omega) = -u^2\sigma(-u^2) = (u\sigma(u))^2$. Suppose $\pi^{2k}(1) = v^2$. Then

$$\pi^{2(k+1)}(1) = \pi^2(v^2) = u^2\sigma\left(u^2\sigma(v^2)\right) = u^2\sigma(u\sigma(v))^2 = \left(u\sigma(u\sigma(v))\right)^2 .$$

Thus the orbit of 1 under the action of $\langle \pi^2 \rangle$ is a subset of S. Since $\langle \pi \rangle = \langle \pi^2 \rangle$ the same must be true of the orbit of 1 under $\langle \pi \rangle$. In particular, $\pi(1) = -u^2(1) = -u^2$ is in S, so $\pi(1) = z^2$. Hence $(-1) = (zu^{-1})^2$, so $4 \mid (p^n-1)$, a contradiction since $(p^n-1)/2$ is odd.

REMARK. If, in T, $O(0) = -S$ then we may define a new tournament T' on the points of $GF(p^n)$ by the rule $a > b$ in T' iff $-a > -b$ in T. Clearly T and T' are isomorphic tournaments so we may suppose that, in T, $O(0) = \{x^2 \mid x \in GF(p^n)^*\}$. We may now prove Theorem A.

Proof of Theorem A. By Theorem 5 we may identify the points of T with those of $GF(p^n)$ so that $A(T)$ is a subgroup K of $\Gamma(p^n)$. By Theorem 6 and the remark after it we may assume $O(0) = \{x^2 \mid x \in GF(p^n)^*\}$. Now if $a, b \in GF(p^n)$ then, since by Theorem 5, K contains all translations in $\Gamma(p^n)$, $a > b$ iff $0 > b - a$, that is, $b - a = x^2$ for some $x \in GF(p^n)^*$. To prove the last statement is now easy, for $A(T)$ is a subgroup of $\Gamma(p^n)$ and $b - a$ and $[x, \sigma, c](b) - [x, \sigma, c](a)$ are both in S or both in $-S$ iff $x \in S$.

References

[1] Walter Feit and John G. Thompson, "Solvability of groups of odd order", *Pacific J. Math.* 13 (1963), 775-1029.

[2] Myron Goldberg, "The group of the quadratic residue tournament", *Canad. Math. Bull.* 13 (1970), 51-54.

[3] B. Huppert, *Endliche Gruppen I* (Die Grundlehren der mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[4] Donald Passman, *Permutation groups* (W.A. Benjamin, New York, Amsterdam, 1968).

Simon Fraser University,
Burnaby,
British Columbia,
Canada.

https://doi.org/10.1017/S0004972700044257 Published online by Cambridge University Press