Michigan Math. J. 58 (2009)

On Generalized Paley Graphs and Their Automorphism Groups

Tian Khoon Lim & Cheryl E. Praeger

Dedicated to the memory of Donald G. Higman

1. Introduction

The generalized Paley graphs are, as their name suggests, a generalization of the Paley graphs, first defined by Paley in 1933 (see [15]). They arise as the relation graphs of symmetric cyclotomic association schemes. However, their automorphism groups may be much larger than the groups of the corresponding schemes. We determine the parameters for which the graphs are connected, or equivalently, the schemes are primitive. Also we prove that generalized Paley graphs are sometimes isomorphic to Hamming graphs and consequently have large automorphism groups, and we determine precisely the parameters for this to occur. We prove that in the connected, non-Hamming case, the automorphism group of a generalized Paley graph is a primitive group of affine type, and we find sufficient conditions under which the group is equal to the one-dimensional affine group of the associated cyclotomic association scheme. The results have been applied in [11] to distinguish between cyclotomic schemes and similar twisted versions of these schemes in the context of homogeneous factorizations of complete graphs.

Let $\mathbb{F}_q$ be a finite field with q elements such that $q \equiv 1 \pmod 4$. Let ω be a primitive element in $\mathbb{F}_q$ and S the set of nonzero squares in $\mathbb{F}_q$, so $S = \{\omega^2, \omega^4, \dots, \omega^{q-1} = 1\} = -S$. The *Paley graph,* denoted by $\mathrm{Paley}(q)$, is the graph with vertex set $\mathbb{F}_q$ and edges all pairs $\{x, y\}$ such that $x - y \in S$. The class of Paley graphs is one of the two infinite families of self-complementary arc-transitive graphs characterized by Peisert in [16]. Moreover, Paley graphs are also examples of distance-transitive graphs, of strongly regular graphs, and of conference graphs; see [8, Sec. 10.3]. The automorphism group $\mathrm{Aut}(\mathrm{Paley}(q))$ of $\mathrm{Paley}(q)$ is of index 2 in the affine group $\mathrm{A\Gamma L}(1, q)$, and each permutation in $\mathrm{A\Gamma L}(1, q) \setminus \mathrm{Aut}(\mathrm{Paley}(q))$ interchanges $\mathrm{Paley}(q)$ and its complementary graph. The generalized Paley graphs are defined similarly.

Definition 1.1 (Generalized Paley graph). Let $\mathbb{F}_q$ be a finite field of order q, and let k be a divisor of $q-1$ such that $k \geq 2$; and if q is odd, then in addition $\frac{q-1}{k}$ is even. Let S be the subgroup of order $\frac{q-1}{k}$ of the multiplicative group $\mathbb{F}_q^*$. Then the *generalized Paley graph* $\mathrm{GPaley}\big(q, \frac{q-1}{k}\big)$ of $\mathbb{F}_q$ is the graph with vertex set $\mathbb{F}_q$ and edges all pairs $\{x, y\}$ such that $x - y \in S$.

Received December 14, 2006. Revision received June 29, 2007.