GOLD AND KASAMI-WELCH FUNCTIONS, QUADRATIC FORMS, AND BENT FUNCTIONS

JYRKI LAHTONEN
Department of Mathematics
University of Turku
20014 Turku, Finland

GARY McGUIRE
School of Mathematical Sciences
University College Dublin
Dublin 4, Ireland

HAROLD N. WARD
Department of Mathematics
University of Virginia
Charlottesville, VA 22904, USA

(Communicated by Patrick Sole)

Abstract. We use elementary facts about quadratic forms in characteristic 2 to evaluate the sign of some Walsh transforms in terms of a Jacobi symbol. These results are applied to the Walsh transforms of the Gold and Kasami-Welch functions. We prove that the Gold functions yield bent functions when restricted to certain hyperplanes. We also use the sign information to determine the dual bent function.

1. Introduction

Let \( K = \mathbb{F}_q \), the finite field with \( q = 2^n \) elements. Let \( \text{Tr} \) denote the trace map from \( K \) to \( \mathbb{F}_2 \). For a Boolean function \( f : K \rightarrow \mathbb{F}_2 \), the Walsh transform (or Walsh-Hadamard transform) of \( f \) is the function \( f^W : K \rightarrow \mathbb{Z} \) defined by
\[
f^W(a) = \sum_{x \in K} (-1)^{f(x) + \text{Tr}(ax)}.
\]
The Walsh transform of \( f \) is the same as the Fourier transform of \((-1)^f\). The Walsh spectrum of \( f \) is the set of values of \( f^W \), the set \( \{f^W(a) : a \in K\} \). Bent functions are functions whose Walsh spectrum is \( \{\pm 2^{n/2}\} \). The most famous examples of functions whose Walsh spectrum has order 3 are the Gold functions \( f(x) = \text{Tr}(x^{2^k+1}) \) where \( k \) is relatively prime to \( n \) and \( n \) is odd. The spectrum here is \( \{0, \pm 2^{(n+1)/2}\} \). Almost as famous are the Kasami-Welch functions \( f(x) = \text{Tr}(x^{4^k-2^k+1}) \), which have the same spectrum under the same hypotheses. In this article we will be concerned with the precise value of \( f^W(1) \), including the sign. We will determine this value for the Gold and Kasami-Welch functions as an application of a more general theorem.