Exact divisibility of exponential sums associated to elementary symmetric Boolean functions

Oscar E. González, Raúl E. Negrón, Francis N. Castro, Luis A. Medina and Ivelisse M. Rubio

Department of Computer Science, University of Puerto Rico at Río Piedras
Department of Mathematics, University of Puerto Rico at Río Piedras

Abstract

An n-variable Boolean function F is a function defined over $\mathbb{F}^n$ with values in $\mathbb{F}$, the finite field with two elements. Our aim is to calculate the exact 2 divisibility of exponential sums associated to Boolean functions. This allows us to determine whether a Boolean function is balanced, i.e. whether $|\{x \in \mathbb{F} | f(x) = 1\}| = 2^{n-1}$, which can be difficult in general. We prove two theorems which give affirmative answers to some of the open cases of Cusick-Li-Stănică's conjecture about the non-existence of certain balanced Boolean funtions.

Preliminaries

Lucas' Theorem

Let $n \in \mathbb{N}$ with 2-adic expansion $n = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_l}$. The binomial coefficient $\binom{n}{k}$ is odd if and only if k is either 0 or a sum of some of the 2^{a_i}'s. □

Notation

- $\mathbb{F}$: the finite field with two elements.
- $\sigma_{n,k}$: $\sigma_k(X_1, \ldots, X_n)$, the elementary symmetric polynomial in n variables of degree k.
- $\nu_2(m)$: The highest power of two that divides the non-zero integer m.
- $w_2(x)$: the Hamming weight of $x \in \mathbb{F}$.
- $k_1 \preceq k_2$: Each 1 appearing in the binary expansion of k_1 also appears in the binary expansion of k_2 for $k_1, k_2 \in \mathbb{N}$.

An important property of ν_2 is that $\nu_2(m+n) \geq \min\{\nu_2(m), \nu_2(n)\}$. Moreover, if $\nu_2(m) \neq \nu_2(n)$, then $\nu_2(m+n) = \min\{\nu_2(m), \nu_2(n)\}$.
Let $F(\mathbf{X}) = F(X_1, \ldots, X_n)$ be a polynomial in n variables over $\mathbb{F}$. **The exponential sum** associated to F over $\mathbb{F}$ is:

$$S(F) = \sum_{x_1,\ldots,x_n \in \mathbb{F}} (-1)^{F(x_1,\ldots,x_n)}$$

Note that F is balanced if and only if $S(F) = 0$. Also note that if $\nu_2(S(\sigma_{n,k})) < \infty$, then the function is not balanced.

Preliminaries

Define A_j to be the set of all $(x_1, \cdots, x_n) \in \mathbb{F}^n$ with exactly j entries equal to 1. Then, $|A_j| = \binom{n}{j}$ and $\sigma_{n,k}(\mathbf{x}) = \binom{j}{k}$ for $\mathbf{x} \in A_j$. This allows us to write the exponential sum associated to an elementary symmetric polynomial in a way that is much more useful for our goals of studying the exact 2 divisibility of such sums.

Exponential sums associated to Boolean functions

In the case of an elementary symmetric polynomial, the exponential sum can be written as

$$S(\sigma_{n,k}) = 2^n - 2 \sum_{j \in N(n,k)} \binom{n}{j},$$

where $N(n,k) = \{0 \leq j \leq n \,|\, \binom{j}{k} \equiv 1 \bmod 2\}$. Thus,

$$\nu_2(S(\sigma_{n,k})) = \nu_2\Big(2 \sum_{j \in N(n,k)} \binom{n}{j}\Big)$$

Previous work

In [2], Cusick, Li and Stănică proposed a conjecture that explicitly states when an elementary symmetric function is balanced:

There are no nonlinear balanced elementary symmetric Boolean functions except for degree $k = 2^l$ and $2^{l+1}D - 1$-variables, where l, D are positive integers.

- There have been various articles which tackle parts of this conjecture, for example [3] in which Cusick, Li and Stănică proved their conjecture for elementary symmetric functions of odd degree and [1] where Castro and Medina proved an asymptotic version of the conjecture.
- Su, Tang and Pott presented the known results about the conjecture, and restated the conjecture to include only the open cases in [4].

Open cases of Cusick-Li-Stănică's Conjecture ([4])

Let $D \geq 3$ be odd, $a \geq 1$, $n = 2^{a+1}D + r$, $r = -1, 0, 1, 2$. The elementary symmetric Boolean function $\sigma_k(X_1, \ldots, X_n)$ is not balanced in the following cases:

1. $k = 2^{a+1}d'$, $w_2(d') \geq 2$, and $2 \leq d' \preceq \frac{D-1}{2}$ for $r = -1, 0, 1, 2$.
2. $k = 2^{a+1}d' + 2^a$, $w_2(d') \geq 2$, and $2 \leq d' \preceq \frac{D-1}{2}$ for $r = 0, 1, 2$.

Problem

We are interested in finding families of elementary symmetric Boolean functions whose exponential sum is not equal to 0 and whose 2-adic valuation can be calculated by elementary methods. Of particular interest are families which are part of the remaining open cases of Cusick-Li-Stănică's conjecture. We study the following families:

- degree $2^a(2^{i-2} - 1)$ and $2^a(2^i - 1)$ variables,
- degree $2^a(2^{i-3} - 1)$ and $2^a(2^i - 1)$ variables,
- degree $2^a m$ and $2^a(2^i + m)$ variables,

where $a, i \in \mathbb{N}$ and m is an odd positive number.

Results

Theorem

Let a, i be natural numbers with $i \geq 6$ and $a \geq 1$. Suppose that $n = 2^a(2^i - 1)$ and $k = 2^a(2^{i-2} - 1)$. Then, $\nu_2(S(\sigma_{n,k})) = 7$. □

Example: Let $i = 6$ and $a = 1$. Then we have that $n = 2(2^6 - 1) = 508$ and $k = 2(2^4 - 1) = 30 = (11110)_2$. By Lucas' Theorem $N(126, 30) = \{30, 31, 62, 63, 94, 95, 126\}$. Using any computer algebra system, we can calculate $2^{126} - 2\sum_{j \in N(126,30)} \binom{126}{j} = 61119442732692689995146730716611952512$ and obtain $\nu_2(S(\sigma_{n,k})) = 7$, as predicted by the theorem.

Theorem

Let a, i be natural numbers with $i \geq 16$ and $a \geq 1$. Suppose that $n = 2^a(2^i - 1)$ and $k = 2^a(2^{i-3} - 1)$. Then, $\nu_2(S(\sigma_{n,k})) = 15$. □

We use Lucas' theorem to determine which elements will be in $N(n,k)$. After conjecturing the value of $\nu_2(S(\sigma_{n,k})) = l$ via computer experiments, we consider the binomials in the sum $\Sigma_{j \in N(n,k)} \binom{n}{j}$ which have 2-adic valuation smaller than l. Note that since $\nu_2(m+n) = \min\{\nu_2(m), \nu_2(n)\}$ for $\nu_2(m) \neq \nu_2(n)$, then to obtain that $\nu_2(S(\sigma_{n,k})) = l$ it is enough to consider these binomials and show that the 2-adic valuation of their sum is $l - 1$. **Our two theorems give affirmative answers to some of the open cases of Cusick-Li-Stănică's Conjecture.**

References

[1] F. N. Castro and L. A. Medina. Linear recurrences and asymptotic behavior of exponential sums of symmetric Boolean functions. *Elec. J. Combinatorics*, 18, 2011.

[2] T. W. Cusick, Yuan Li, and P. Stănică. Balanced symmetric functions over $GF(p)$. *IEEE Trans. on Information Theory*, 5:1304–1307, 2008.

[3] T. W. Cusick, Yuan Li, and P. Stănică. On a conjecture for balanced symmetric Boolean functions. *J. Math. Crypt.*, 3:1–18, 2009.

[4] W. Su, X. Tang, and A. Pott. A note on a conjecture for balanced elementary symmetric Boolean functions. *IEEE Trans. on Information Theory*, 59:665–671, 2013.

Acknowledgements

This research was supported by a National Science Foundation grant (DMS1148695) through the Center for Undergraduate Research (CURM), Brigham Young University, and corporate sponsors. Also, partial support was provided to the students by the Claude Shannon Scholarship, NSF-UPR-RP-Scholarship fund for excellence in Computer Science and Mathematics, (NSF-DUE 1356474).