Comments on "Generating and Counting Binary Bent Sequences"

Claude Carlet

INRIA Rocquencourt, Domaine de Voluceau
Bat 10, BP 105, 78153 Le Chesnay Cedex, France
Université de Picardie, France

Jennifer Seberry
and
Xian-Mo Zhang

Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522, Australia

Abstract

We prove that the conjecture on bent sequences stated in "Generating and counting bent sequences", IEEE Transactions on Information Theory, IT-36 No. 5, 1990 by C.M. Adams and S.E. Tavares is false.

Let V_n be the vector space of n tuples of elements from $GF(2)$. Any map from V_n to $GF(2)$, f, can be uniquely written as a polynomial in coordinates x_1, ..., x_n [3], [4]:

$$f(x_1, \ldots, x_n) = \bigoplus_{v \in V_n} a_v x_1^{v_1} \cdots x_n^{v_n}$$

where $\oplus$ denotes the boolean addition, $v = (v_1, \ldots, v_n)$, $a_v \in GF(2)$. Thus we identify the function f with polynomial f. Note that there exists a natural one to one correspondence between vectors in V_n and integers in $\{0, 1, \ldots, 2^n - 1\}$. This allows us to order all the vectors according to their corresponding integer values. For convenience, we use α_i to denote the vector in V_n whose integer representation is i. Let f be a function on V_n. The $(1, -1)$-sequence

$$(-1)^{f(\alpha_0)},\ (-1)^{f(\alpha_1)},\ \ldots\ ,(-1)^{f(\alpha_{2^n-1})}$$

is called the *sequence* of $f(x)$.

The function $\varphi(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, a_j, $c \in GF(2)$, is called an *affine function,* on V_n, in particular, a *linear function* if $c = 0$. The sequence of an affine (a linear) function is called an *affine sequence* (a *linear sequence*).

From [4] we can give an equivalent definition of bent functions. Let ξ be the sequence of a function f on V_n. We call f a *bent function* and ξ a *bent sequence*, if the scalar product

$\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any linear sequence ℓ of length 2^n. Obviously bent functions on V_n exist only for even n.

Consider all the $(1,-1)$-sequences of length four: $\pm(++++)$, $\pm(++--)$, $\pm(+-+-)$, $\pm(+--+)$, $\pm(+++-)$, $\pm(++-+)$, $\pm(+-++)$, $\pm(-+++)$, where $+$ and $-$ denote 1 and -1 respectively. Each of the first eight is an affine sequence. For example, $(-++-)$ is the sequence $\varphi(x_1,x_2) = 1 \oplus x_1 \oplus x_2$: $(-1)^{\varphi(0,0)} = -1$, $(-1)^{\varphi(0,1)} = 1$, $(-1)^{\varphi(1,0)} = 1$, $(-1)^{\varphi(1,1)} = -1$. Note that a function on V_2 is bent if and only if it is quadratic. Thus each of the second eight is a bent sequence. For example, $(--+-)$ is the sequence $g(x_1,x_2) = 1 \oplus x_1 \oplus x_1x_2$: $(-1)^{g(0,0)} = -1$, $(-1)^{g(0,1)} = -1$, $(-1)^{g(1,0)} = 1$, $(-1)^{g(1,1)} = -1$.

If a bent sequence of length 2^n is a concatenation of 2^{n-2} bent (affine) sequences of length 4 we call it *bent-based* (*linear-based*) *bent sequence*. Adams and Tavares conjectured that any bent sequence is either bent-based or linear-based [1]. We now prove that this conjecture is true if only if any bent function is quadratic. However there exist infinitely many bent functions with algebraic degree higher than two [2], [4]. This implies that the conjecture is not true.

The next lemma follows directly from the definition of bent-based (linear-based) bent sequences.

Lemma 1 *Let ξ be the sequence of a bent function, f, on V_n ($n > 2$). Then ξ is bent-based (linear-based) if and only if $f(x_1^0, \ldots, x_{n-2}^0, x_{n-1}, x_n)$ is a bent (an affine) function on V_2 for any fixed vector $(x_1^0, \ldots, x_{n-2}^0) \in V_{n-2}$.*

Note that any function on V_n can be written as

$$\begin{aligned} f(x_1,\ldots,x_n) &= r(x_1,\ldots,x_{n-2}) \oplus p(x_1,\ldots,x_{n-2})x_{n-1} \oplus q(x_1,\ldots,x_{n-2})x_n \\ &\oplus \; a(x_1,\ldots,x_{n-2})x_{n-1}x_n \end{aligned} \qquad (1)$$

where p, q, r and a are functions on V_{n-2}. From Lemma 1, it is easy to verify

Lemma 2 *Let ξ be the sequence of a bent function, f, on V_n ($n > 2$). Then ξ is bent-based (linear-based) if and only if $a(x_1, \ldots, x_{n-2})$ is the constant 1 (constant 0) in the expression for f in (1).*

Theorem 1 *The conjecture of Adams and Tavares is true if only if every bent function is quadratic.*

Proof. Let ξ be the sequence of an arbitrary bent function on V_n ($n > 2$), say f.

Suppose any bent function is quadratic. It is easy to see that $a(x_1, \ldots, x_{n-2})$ is constant in the expression for f as in (1). By Lemma 2, the conjecture is true.

Conversely, suppose the conjecture is true i.e. ξ is either bent-based or linear based. By Lemma 2, $a(x_1, \ldots, x_{n-2})$ is constant in the expression for f as in (1). Suppose f is not quadratic. Then there exist two distinct indices i and j such that the coefficient of $x_i x_j$ in the expression for f is not constant. Rewrite $f(x_1, \ldots, x_n) = g(x_{j_1}, \ldots, x_{j_{n-2}}, x_i, x_j)$, where $j_1, \ldots, j_{n-2}$ is any permutation of $\{1, \ldots, n\} - \{i, j\}$. Applying the conjecture to g leads a contradiction.

□

References

[1] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, IT-36 No. 5:1170–1173, 1990.

[2] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory*, Ser. A, 40:90–107, 1985.

[3] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* New York: North-Holland, 1977.

[4] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.