Divisibility of the Hamming Weight by 2^k and Monomial Criteria for Boolean Functions

Dmitry Khovratovich, diho@rnt.ru

Moscow State University, Faculty of Computational Mathematics and Cybernetics

Abstract. In this paper we consider the notions of the Hamming weight and the algebraic normal form. We solve an open problem devoted to checking divisibility of the weight by 2^k. We generalize the criterion for checking the evenness of the weight in two ways. Our main result states that for checking whether the Hamming weight of f is divisible by 2^k, $k > 1$, it is necessary and sufficient to know its algebraic normal form accurate to an additive constant.

Keywords: boolean functions, Hamming weight, algebraic normal form, coding theory.

1 Introduction

In this paper we consider the notion of the weight of a boolean function. We solve an open problem from [1]: we formulate criteria for divisibility of the weight by powers of two.

In the sequel, the following notation will be used (see, i.e. [3]). A *boolean function f of n variables* is a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2$. It can be expressed as a polynomial, called its *algebraic normal form* (ANF):

$$f(x) = \bigoplus_{\alpha \in \mathbf{F}_2^n} c_\alpha x^\alpha, \quad c_\alpha \in \mathbf{F}_2, \tag{1}$$

where $\oplus$ denotes the addition over $\mathbf{F}_2$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.

Denote by $\mathrm{wt}(f)$ *the (Hamming) weight* of f, i.e. the size of the set $N_f \stackrel{\text{def}}{=} \{x \in \mathbf{F}_2^n | f(x) = 1\}$. We say that $\mathrm{wt}(f)$ *is divisible by t* if $\mathrm{wt}(f) \equiv 0 \pmod t$.

As noticed in [1], divisibility of $\mathrm{wt}(f)$ by 2^k for some k is a property of a function that is useful in coding theory. Assume we know the ANF of f (1). Then it may be proved that

Proposition 1 ([1]). *The weight of f is divisible by 2 iff* $c_{(1,1,\ldots,1)} = 0$.

Hence we do not need to know all c_α. Logachev et al. [1] set a problem: can this property be somehow extended to other divisors of the form 2^k?

They also conjectured that the following theorem by McEliece could be generalized with respect to the set of all non-zero ANF coefficients.

Proposition 2 ([2]). *Suppose f is a boolean function, and its algebraic normal form is a polynomial of degree r. Then* $\mathrm{wt}(f)$ *is divisible by* $2^{\lceil m/r \rceil - 1}$.

2 The main result of the paper

We find the relationship between the set of non-zero coefficients of algebraic normal form and divisibilty of the weight by 2^k. We generalize the proposition 1 in two ways. We consider both ways and show that only trivial criteria may be formulated.

3 First generalization

Denote by C_f the set of all α giving non-zero coefficients in the ANF (1). Also denote $(11\dots1)$ by $\mathbf{1}$ and$(00\dots0)$ by $\mathbf{0}$. With respect to this notation we obtain

$$\mathrm{wt}(f) \equiv 0 \pmod 2 \;\Leftrightarrow\; C_f \subseteq \mathbf{F}_2^n \setminus \{\mathbf{1}\}. \tag{2}$$

from Pr. 1.

Let us give an appropriate definition.

We say that a set $G \subset \mathbf{F}_2^n$ is a *strongly criterial with respect to the property* $\mathfrak{C}$ if for any $f \in \mathbf{F}_n$ the following condition holds:

$$f \text{ has } \mathfrak{C} \iff C_f \subseteq G.$$

One may assume that such a condition is too strong. Indeed, we have the following theorem.

Theorem 1. *Suppose k is a positive integer and not greater than n. Then a strongly criterial set with respect to divisibility of the weight by 2^k exists iff $k = 1$ or $k = n$.*

Proof. We consider three cases.

- $k = 1$. Using (2) we obtain that $\mathbf{F}_2^n \setminus \{\mathbf{1}\}$ is a strongly criterial set w.r.t. divisibility of the weight by two.
- $k = n$. We get $\mathrm{wt}(f) \equiv 0 \pmod{2^n}$. Taking into account the fact that $0 \leqslant \mathrm{wt}(f) \leqslant 2^n$ we obtain that f is a constant. Obviously $C_0 = \emptyset$ and $C_1 = \{\mathbf{0}\}$. Denote by G the set $\{\mathbf{0}\}$. It is easy to prove that

  $$\mathrm{wt}(f) \equiv 0 \pmod{2^n} \iff C_f \subseteq G.$$

  This implies that G is strongly criterial.
- $1 < k < n$. Now we show that no strongly criterial set exists for such k. Assume the converse. Let G be a strongly criterial set w.r.t. divisibility of the weight by 2^k. Suppose functions f_1, f_2 satisfy following conditions:

  $$\begin{aligned} \mathrm{wt}(f_1) &\equiv 0 \pmod{2^k}, \\ \mathrm{wt}(f_2) &\equiv 0 \pmod{2^k}. \end{aligned} \tag{3}$$

  Then we have

  $$C_{f_1} \subseteq G,\; C_{f_2} \subseteq G \implies G \supseteq C_{f_1} \cup C_{f_2} \supseteq C_{f_1 \oplus f_2}.$$

  Therefore, we have

  $$\mathrm{wt}(f_1 \oplus f_2) \equiv 0 \pmod{2^k}. \tag{4}$$

  To get a contradiction, we construct functions f_1 and f_2 which satisfy (3) and do not satisfy (4).

  Indeed, the condition $1 < k < n$ implies the following. The reader will easily prove that there exist sets $A_1, A_2 \subset \mathbf{F}_2^n$ such that

  $$|A_1| = |A_2| = 2^k, \quad |(A_1 \cap A_2)| = 1.$$

  Now we define f_1 and f_2. By definition, put

  $$f_i(x) = 1 \;\Leftrightarrow\; x \in A_i, \quad i = 1, 2.$$

  We obtain

  $$\begin{aligned} |N_{f_1}| = |N_{f_2}| = 2^k &\equiv 0 \pmod{2^k}; \\ |N_{f_1 \oplus f_2}| = |(A_1 \triangle A_2)| = 2 \cdot 2^k - 2 &\not\equiv 0 \pmod{2^k}. \end{aligned}$$

  Therefore, f_1 and f_2 satisfy (3) and do not satisfy (4). This contradiction proves the theorem.

Therefore, our generalization implies too strong conditions. Let us make them weaker.

4 Second generalization

We say that a set $G \subset \mathbf{F}_2^n$ is a *weakly criterial with respect to the property* $\mathfrak{C}$, if for any f_1 and f_2 the condition

$$\text{Either } f_1 \text{ or } f_2 \text{ has } \mathfrak{C}$$

implies

$$G \cap C_{f_1} \neq G \cap C_{f_2}.$$

We will omit the phrase ¡¡with respect to $\mathfrak{C}$¿¿ when $\mathfrak{C}$ is clear from context.

Example. Using (2) we obtain that the set $\{\mathbf{1} = (1, 1, \ldots, 1)\}$ is a weakly criterial w.r.t. divisibility of the weight by 2.

Let us remark that such a definition is actually weaker than the former one. Any weakly criterial set only divides the set of all boolean functions into equivalence classes: $M_1 \sim M_2 \Leftrightarrow G \cap M_1 = G \cap M_2$.

We claim that there exist only trivial weakly criterial sets.

Theorem 2. *Let k be a positive integer such that $2 \leqslant k \leqslant n$. Then for the set G to be weakly criterial w.r.t. divisibility of the weight by 2^k it is necessary and sufficient to have $(\mathbf{F}_2^n \setminus \{\mathbf{0}\}) \subseteq G$.*

Proof. First of all, we prove sufficiency. Secondly, we prove necessity for $k = n$. Finally, we prove necessity for $2 \leqslant k \leqslant n - 1$.

Sufficiency. Let G be a set of n-tuples such that $(\mathbf{F}_2^n \setminus \{\mathbf{0}\}) \subseteq G$. Then only two cases are possible: $G = \mathbf{F}_2^n$ and $G = \mathbf{F}_2^n \setminus \{\mathbf{0}\}$.

The first case is trivial: obviously, $\mathbf{F}_2^n$ is a weakly criterial set. Consider the second case.

Let f be a boolean function such that

$$\mathrm{wt}(f) \equiv 0 \pmod{2^k}. \tag{5}$$

Now we prove that $G = \mathbf{F}_2^n \setminus \{\mathbf{0}\}$ is a weakly criterial set.

Assume the converse: there exists a function f' such that

$$\mathrm{wt}(f') \not\equiv 0 \pmod{2^k}, \tag{6}$$

but

$$G \cap C_f = G \cap C_{f'}. \tag{7}$$

Hence we have

$$G = \mathbf{F}_2^n \setminus \{\mathbf{0}\} \implies G \cap C_f = C_f \setminus \{\mathbf{0}\},\ G \cap C_{f'} = C_{f'} \setminus \{\mathbf{0}\}.$$

If we combine this with (6), we get

$$C_f \setminus \{\mathbf{0}\} = C_{f'} \setminus \{\mathbf{0}\}. \tag{8}$$

It implies that the ANF of f equals the ANF of f' accurate to a constant. Using the condition $f \neq f'$ we get $f' = f \oplus 1$. It is easy to prove that $\mathrm{wt}(f) + \mathrm{wt}(f \oplus 1) = 2^n$ for any f. Combining it with (5) and the condition $k \leqslant n - 1$, we obtain $\mathrm{wt}(f') \equiv 0 \pmod{2^k}$. It implies the contradiction with (7).

Thus G is a weakly criterial set of tuples.

Necessity for $k = n$. By definition, put $f_1 \equiv 0$ and $f_2 = \mathrm{x}^a$, where a is an arbitrary non-zero tuple. Then the following conditions hold:

$$f_1 \text{ has the property of } 2^n\text{-divisibility;}$$
$$f_2 \text{ does not have the property of } 2^n\text{-divisibility;}$$
$$C_{f_1} = \emptyset,\ C_{f_2} = \{a\}.$$

Take any weakly criterial set G with respect to divisibility of the weight by 2^k. This implies

$$G \cap C_{f_1} \neq G \cap C_{f_2}.$$

Hence we obtain $G \cap C_{f_2} = \{a\}$. Arbitrariness of a implies

$$(\mathbf{F}_2^n \setminus \{\mathbf{0}\}) \subseteq G.$$

Necessity for $2 \leqslant k \leqslant n-1$. Let k belongs to $[2; n-1]$ and let G be a weakly criterial set w.r.t. divisibility of the weight by 2^k. Now we prove that $(\mathbf{F}_2^n \setminus \{\mathbf{0}\}) \subseteq G$.

Assume the converse: $(\mathbf{F}_2^n \setminus \{\mathbf{0}\}) \nsubseteq G$. Fix an arbitrary tuple $\alpha \in \mathbf{F}_2^n \setminus (\{\mathbf{0}\} \cup G)$. Consider two cases.

- $\alpha = \mathbf{1}$. Consider the functions $f_1 \equiv 0$ and $f_2 \equiv \mathrm{x}^\alpha = x_1 x_2 \cdots x_n$. It follows easily that

$$\mathrm{wt}(f_1) \equiv 0 \pmod{2^k};$$
$$\mathrm{wt}(f_2) \equiv 1 \pmod{2^k};$$
$$G \cap C_{f_1} = G \cap C_{f_2} = \emptyset.$$

  Hence G is not a weakly criterial set, so we get a contradiction.
- $\alpha \neq \mathbf{1}$. Denote by A the set $\{a \in \mathbf{F}_2^n \mid \alpha \preccurlyeq a \preccurlyeq \mathbf{1}\}$, where $\alpha \preccurlyeq \beta$ describes the partial ordering on the Boolean lattice. Also denote the number of units (non-zero elements) in α by m. Then we obtain

$$|A| = 2^{n-m},\ m \leqslant n-1,\ |\mathbf{F}_2^n \setminus A| \geqslant 2^{n-1}. \tag{9}$$

  Note that

$$x^\alpha = 1 \Leftrightarrow x \in A. \tag{10}$$

  (9) implies the existence of a function f such that

$$|N_f \cap A| = 2^{n-m-1} - 1,\ |N_f \setminus A| = 2^{n-1} - 2^{n-m-1} + 1. \tag{11}$$

  Fix an arbitrary f that satisfies (11). Define a function f' by the rule

$$f' = f \oplus \mathrm{x}^\alpha.$$

  It implies

$$G \cap C_f = G \cap C_{f'}. \tag{12}$$

  Therefore, we have

$$N_f \setminus A = N_{f'} \setminus A \quad \text{from (10);} \tag{13}$$
$$|N_f \cap A| + |N_{f'} \cap A| = |A|. \tag{14}$$

  Combining (11) with the condition $k \leqslant n-1$, we get

$$\mathrm{wt}(f) = 2^{n-m-1} - 1 + 2^{n-1} - 2^{n-m-1} + 1 = 2^{n-1} \equiv 0 \pmod{2^k}. \tag{15}$$

  To evaluate $\mathrm{wt}(f')$, we combine the equations (13) and (14) with (9) and (11). Then we see that

$$\mathrm{wt}(f') = 2^{n-m} - (2^{n-m-1} - 1) + 2^{n-1} - 2^{n-m-1} + 1 = 2^{n-1} + 2 \equiv 2 \pmod{2^k}. \tag{16}$$

  Therefore, the weight of f' is not divisible by 2^k, which is contrary to (12). This contradiction proves the theorem.

5 Summary

Hence for checking whether the Hamming weight of f is divisible by 2^k, $k > 1$, it is necessary and sufficient to know its algebraic normal form accurate to an additive constant.

The author is grateful to professors Alekseev V.B. and Logachev O. A. for constant attention to this work.

This research was partially supported by RFBR grant 06-01-10023.

References

1. O. A. Logachev, A. A. Salnikov, V. V. Yaschenko *"Boolean functions in coding theory and cryptology"*, Moscow, MCCME, 2004 (In Russian).
2. R. J. McEliece *"Weight congruences for p-ary cyclic codes"*, Discrete Math 3 (1972), pp 177–192.
3. A. Canteaut, E. Filiol, *"Ciphertext Only Reconstruction of Stream Ciphers Based on Combination Generators"*, FSE 2000, number 3027 in Lecture Notes in Computer Science, pages 165–180. Springer-Verlag, 2000.