Estimating the nonlinearity of Boolean functions using probabilistic linearity tests

Ana Sălăgean
Department of Computer Science,
Loughborough University, UK
A.M.Salagean@lboro.ac.uk

Pantelimon Stănică
Applied Mathematics Department,
Naval Postgraduate School, Monterey, USA
pstanica@nps.edu

Abstract

In this paper we concentrate on estimating the nonlinearity of Boolean functions, by probabilistic methods, when it is not feasible to compute the full Walsh transform. Firstly, we improve upon the bounds on the probabilities of failure of existing affinity tests. Secondly, we provide probabilistic tests for estimating nonlinearity based upon either affinity tests or linearity tests (such as the BLR test) and analyze the accuracy of the estimation.

Keywords: nonlinearity, Walsh transform, probabilistic testing

1 Introduction

Boolean functions are functions defined on a vector space over the finite field $\mathbb{F}_2$. For many cryptographic applications it is important that functions are not affine, and not even close to being affine. The nonlinearity of a function f, denoted $\mathrm{d}_{\mathcal{A}}(f)$, defined as the least Hamming distance to any affine function, is therefore an important indicator in cryptography. This indicator can be computed by using the Walsh transform (also called Walsh-Hadamard or discrete Fourier transform). The Walsh transform of a function f in n variables is typically computed starting from the truth table of f and using a $\mathcal{O}(2^n)$ algorithm similar to the fast Fourier transform. Computing the Walsh transform is not feasible in practice when the number of variables is large (e.g. at least 80 variables for typical cryptographic applications) and the function is given as a "black box" (or given by an algorithm/formula which is not amenable to simple manipulation for the purpose of computing the Walsh transform).

The motivation of this paper is to probabilistically estimate the nonlinearity of f, to a reasonable degree of accuracy. The main idea is as follows. Consider a probabilistic test which has a success/fail outcome based on the values of f at some fixed number k of points in $\mathbb{F}_2^n$ (f can therefore be given as a "black box" function). We will see concrete examples of tests shortly, namely certain tests that are usually used for testing whether a

function is linear or affine; other tests might also work. Denote by $P_T(f)$ the probability of failing the test (the probability over all possible choices of k inputs in $\mathbb{F}_2^n$). We assume $P_T(f)$ is positively correlated, to some extent, with the nonlinearity $\mathrm{d}_{\mathcal{A}}(f)$ and can be bounded by some functions in $\mathrm{d}_{\mathcal{A}}(f)$:

$$\mathrm{Lower}(\mathrm{d}_{\mathcal{A}}(f)) \leq P_T(f) \leq \mathrm{Upper}(\mathrm{d}_{\mathcal{A}}(f)).$$

If we can obtain $P_T(f)$ with reasonable accuracy by practical statistical testing (e.g. binomial proportion confidence interval), we can then estimate the nonlinearity as (we use $F^{-1}(x)$ to denote the preimage of x under F):

$$\mathrm{d}_{\mathcal{A}}(f) \in [\min(\mathrm{Upper}^{-1}(P_T(f))), \max(\mathrm{Lower}^{-1}(P_T(f)))], \tag{1}$$

or, if the preimage has only one element

$$\mathrm{d}_{\mathcal{A}}(f) \in [\mathrm{Upper}^{-1}(P_T(f)), \mathrm{Lower}^{-1}(P_T(f))]. \tag{2}$$

To obtain an accurate estimate, it is important that $P_T(f)$ depends strongly on $\mathrm{d}_{\mathcal{A}}(f)$ and that the bounds are tight. We will examine several probabilistic tests, improve some of the bounds and analyze the accuracy of the resulting estimation.

The linearity test most commonly used is based on the textbook definition of a linear function, namely $f(x+y)+f(x)+f(y)=0$ (often called the BLR test as it was used in [3]): what it means is that we pick randomly $x, y \in \mathbb{F}_2^n$, compute $x+y$, query the black box to extract $f(x), f(y), f(x+y)$ and check if the mentioned linearity holds. If a function passes this test for many pairs (x, y) (chosen uniformly at random) then the function is probably linear. If it fails at least one of the tests then we know the function is not linear. We denote by $\mathrm{P}_2(f)$ the probability of f failing the test (probability taken over all pairs $(x, y) \in \mathbb{F}_2^{2n}$) and the normalized Hamming distance of f to the closest linear function, by $\mathrm{d}_{\mathcal{L}}(f)$. Several authors have determined upper and lower bounds for $\mathrm{P}_2(f)$ as a function of $\mathrm{d}_{\mathcal{L}}(f)$ (see [1, 8] and the references therein).

For cryptographic applications we are not so much interested in whether the function is linear, but rather whether it is affine. For example, such tests play a crucial role in the cube and AIDA attacks (see [5, 9]), which are refined high-order differential attacks, targeted at primitives in stream and block ciphers based on low-degree components. The test used in the cube attack [5] for checking whether a function f is affine is to check whether $f(x+y)+f(x)+f(y)+f(0)=0$ holds (for randomly chosen x, y), which can be viewed as using the BLR test to check whether $f(x)-f(0)$ is linear. The attack starts with a "black box" cryptographic Boolean function $g(v_1, \ldots, v_s, k_1, \ldots, k_m)$ where the k_i are the secret variables such as the bits of the secret key and the v_i public variables are bits that can be manipulated by the attacker, such as the initialisation vector of a stream cipher. For example, in the attack on the stream cipher Trivium in [5, 9], g describes the first bit of the keystream as a function of the public 80 bits of the initialisation vector and the secret 80 key bits. The computation of g starts with some relatively simple functions (of algebraic degree two), which are iteratively composed 1152 times for the full cipher, or about 700 times for reduced versions of the cipher. It is therefore not feasible in practice

to compute the algebraic normal form or the truth table of this function. Instead, g is treated as a "black box" function. During the preprocessing phase (offline phase) of the attack, the attacker can control both the public and the secret variables and constructs several candidate functions in $(k_1, \ldots, k_m)$ (these candidate functions are obtained by choosing, heuristically, a certain subset of the public variables and summing g over all the possible values of those public variables, while keeping the other public variables fixed; equivalently, one computes the higher-order discrete derivative of g with respect to the chosen public variables). Each of these candidate functions is tested in the hope that it is affine. Those that are found to be "probably affine" can later be used in the online phase of the attack, when the key is secret, to construct a linear system of equations, the solution of which reveals the secret key.

Another test usually used in the literature for testing whether a function is affine is to check whether the equation $f(x+y+z)+f(x)+f(y)+f(z) = 0$ holds, for some randomly chosen $x, y, z \in \mathbb{F}_2^n$. Like in the case of the linearity test, if f passes the test many times, then f is probably affine. We denote by $\mathrm{P}_3(f)$ the probability of f failing the affinity test (probability taken over all triplets $(x, y, z) \in \mathbb{F}_2^{3n}$) and denote the normalized Hamming distance of f to the closest affine function, by $\mathrm{d}_{\mathcal{A}}(f)$ (note that this is the nonlinearity of f, in a cryptographic context). As for the linearity tests, we wonder whether $\mathrm{P}_3(f)$ is related to $\mathrm{d}_{\mathcal{A}}(f)$, the distance to the closest affine function. A lower bound was given in Bellare et al. [1].

A generalization of the tests above is proposed in [11], where the authors define the notion of k-th order nonhomomorphicity of a function f as the probability $P_k(f)$ of failing the test $f(x_1 + \cdots + x_k) + f(x_1) + \cdots + f(x_k) = 0$ (probability taken over all tuples $(x_1, \ldots, x_k) \in \mathbb{F}_2^{kn}$). It is shown that for k odd, f is affine if and only if $P_k(f) = 0$; for k even, f is linear if and only if $P_k(f) = 0$; also, still for k even, f is affine if and only if $P_k(f) \in \{0, 1\}$. Bounds on $P_k(f)$ for k odd are given in [11]. The authors also show that the probability of failing these tests can be accurately estimated by statistical methods.

In this paper, we firstly improve both the upper and lower bounds presented in [11] for $P_k(f)$ with k odd, see Section 3. Consequently, we obtain a more precise estimate of the nonlinearity for each given value of $P_k(f)$.

Secondly, we consider the following test for affine functions. We pick any linearity test and run it repeatedly on f and also on $f+1$. If either f or $f+1$ passes the linearity test, then f is probably affine. This idea was mentioned in [11] for their linearity test with k even. However, no results were given regarding how the probability of failing this test depends on the nonlinearity of f. In Section 4 we give such bounds for the probability when the BLR test is used as the linearity test. Our bounds are derived using results from Bellare et al. [1].

The nonlinearity of a function f can be estimated by first using any of the above tests and a practical statistical method to estimate the probability of failing that test. Then, using (1) or (2) we obtain an estimate for the nonlienarity of f. In Section 5 we analyze the accuracy of the estimation. There are functions f, g such that f has higher probability of failing the test than g, even though f has lower nonlinearity than g. This was shown in [2] for the BLR test and in [11] for the tests based on nonhomomorphicity with k odd. However, the estimates get more accurate as k increases. This was noticed in [11], and

our improved bounds lead to an accuracy which increases with k faster than it would if the bounds of [11] were used.

Other nonlinearity tests were proposed for reducing the number of evaluations needed for the black box function, such as [6] and [10] (the latter being also useful for estimating the algebraic degree of f). The further study of the connection between the probability of failing these tests and the nonlinearity will be the subject of further work.

2 Preliminaries

We recall definitions and known results needed for the rest of the paper.

Boolean functions in n variables are functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$. It is well known that any such function can be uniquely represented in its ANF (Algebraic Normal Form), i.e. as a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ of degree at most 1 in each variable. The total degree of the ANF representation is called the *algebraic degree* of f. Functions of algebraic degree one are called affine; affine functions with zero constant term are called linear. We will denote by $\mathcal{A}$ the set of affine functions and by $\mathcal{L}$ the set of linear functions in n variables over $\mathbb{F}_2$.

The Hamming distance between two vectors of the same size is defined as the number of positions where the entries are different. The Hamming weight of a vector is the number of positions where the vector is nonzero. We will use here the normalized distance and weight, i.e. we divide by the length of the vector. Precisely, we define the (normalized) Hamming distance and Hamming weight for vectors $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ in $\mathbb{F}_2^n$, as well as the distance of a vector to a set of vectors S as:

$$\begin{aligned} \mathrm{d}(a, b) &= \frac{1}{k} |\{i : 1 \le i \le k, a_i \ne b_i\}| \\ \mathrm{w}(a) &= \frac{1}{k} |\{i : 1 \le i \le k, a_i \ne 0\}| \\ \mathrm{d}_S(a) &= \min_{s \in S} \mathrm{d}(a, s). \end{aligned}$$

The Hamming weight and distance for Boolean functions are defined as the Hamming weight and distance of their truth tables, where the truth table of a function f is the vector $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$, where v_i are all the elements of $\mathbb{F}_2^n$ in some fixed order, e.g. lexicographical order.

Of particular importance will be the distance of a function f to the set of affine or of linear functions. The minimum distance to any affine function, $\mathrm{d}_{\mathcal{A}}(f)$, is called the *nonlinearity* of f and is a very important cryptographic indicator. It is easy to see that $\mathrm{d}_{\mathcal{A}}(f) = \min(\mathrm{d}_{\mathcal{L}}(f), \mathrm{d}_{\mathcal{L}}(f + 1))$.

The Fourier-Hadamard transform of a function $f : \mathbb{F}_2^n \to \mathbb{R}$ (the 0/1 values of a Boolean functions are viewed as real numbers for this purpose) is the function $W(f) : \mathbb{F}_2^n \to \mathbb{R}$ defined as

$$W(f)(u) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{u \cdot x},$$

where the dot product can be defined as $u \cdot x = \sum_{i=1}^{n} u_i x_i$. Note that we use a normalized version of the transform here. If f is replaced by its sign function, $\hat{f}$, defined by $\hat{f}(x) = (-1)^{f(x)}$, then $W(\hat{f})$ is customarily referred to as the Walsh (or Walsh-Hadamard) transform of f and the values $W(\hat{f})(u)$ for $u \in \mathbb{F}_2^n$ are called the Walsh coefficients. We will refer to the sequence of output values of the Walsh transform (when the input is ordered lexicographically) as the Walsh spectrum.

We will be using later Parseval's identity (see [4] for example):

$$\sum_{u \in \mathbb{F}_2^n} (W(\hat{f})(u))^2 = 1. \tag{3}$$

It is well-known [4] and easy to see that the Walsh transform gives the distances of f to each linear function, and consequently the distance of f to affine functions. Moreover, the nonlinearity of f is related to the Walsh transform as follows ($\ell_a(u) = a \cdot u$ is the linear function corresponding to $a \in \mathbb{F}_2^n$):

$$\begin{aligned} \mathrm{d}(f, \ell_a) &= \frac{1}{2}\left(1 - W(\hat{f})(a)\right) \\ \mathrm{d}(f, \ell_a + 1) &= \frac{1}{2}\left(1 + W(\hat{f})(a)\right) \\ \mathrm{d}_{\mathcal{L}}(f) &= \frac{1}{2}\left(1 - \max_{u \in \mathbb{F}_2^n} W(\hat{f}(u)\right) \\ \mathrm{d}_{\mathcal{A}}(f) &= \frac{1}{2}\left(1 - \max_{u \in \mathbb{F}_2^n} |W(\hat{f})(u)|\right). \end{aligned} \tag{4}$$

Note that $0 \leq \mathrm{d}_{\mathcal{L}}(f) \leq \frac{1}{2}$. It is known that $0 \leq \mathrm{d}_{\mathcal{A}}(f) \leq \frac{1}{2}\left(1 - \frac{1}{2^{\frac{n}{2}}}\right)$. We call a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ ($n \geq 2$) bent if its nonlinearity is exactly $\frac{1}{2}\left(1 - \frac{1}{2^{\frac{n}{2}}}\right)$ (they exist only for even integer n). It is known [4] that f is bent if and only if the Walsh coefficients in absolute value are all $|W(\hat{f})(u)| = 2^{-\frac{n}{2}}$.

The k-th order nonhomomorphicity of a function f, for an integer $k \geq 2$, is defined as the probability $P_k(f)$ that the equation $f(x_1 + \ldots + x_k) + f(x_1) + \cdots + f(x_k) = 0$ does not hold (probability taken over all tuples $(x_1, \ldots, x_k) \in \mathbb{F}_2^{kn}$). Note that this is actually called the $(k+1)$-order nonhomomorphicity in [11], but we adopted the notation from [7], as it seemed more convenient for our purpose. In other words, $P_k(f)$ is the Hamming weight of the function $F : \mathbb{F}_2^{kn} \to \mathbb{F}_2$, $F(x_1, \ldots, x_k) = f(x_1 + \ldots + x_k) + f(x_1) + \cdots + f(x_k)$. Note that the BLR test is the particular case of $k = 2$.

3 Improved bounds on the probability of failure of existing affinity tests

We consider the test of whether a function is affine by checking whether $f(x_1 + \cdots + x_k) + f(x_1) + \cdots + f(x_k) = 0$ for some fixed odd integer k. We examine the relationship between the probability $P_k(f)$ of failing this test and $\mathrm{d}_{\mathcal{A}}(f)$, the nonlinearity of f.

A lower bound for $\mathrm{P}_3(f)$ was proven in [1, Lemma 2.1] (with $x = \mathrm{d}_{\mathcal{A}}(f)$):

$$\begin{aligned}\mathrm{P}_3(f) &\geq \max\left(8x(1-x)\left(\frac{1}{2}-x\right), 2x(1-x)\right)\\ &= \begin{cases} 8x(1-x)\left(\frac{1}{2}-x\right) & \text{if } x \leq \frac{1}{4}\\ 2x(1-x) & \text{if } x > \frac{1}{4}.\end{cases}\end{aligned} \tag{5}$$

The following lower and upper bounds were given in [11] for k odd (we reformulated them to use the normalized version):

$$\frac{1}{2}\left(1 - 2^n\left(1 - 2\,\mathrm{d}_{\mathcal{A}}(f)\right)^{k+1}\right) \leq P_k(f) \leq \frac{1}{2}. \tag{6}$$

We improve on these bounds as follows:

Theorem 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and let $k \geq 2$ be an integer. For k odd we have the following lower and upper bounds for the probability $P_k(f)$ of failure of the test $f(x_1 + \cdots + x_k) + f(x_1) + \cdots + f(x_k) = 0$:*

$$\frac{1}{2}\left(1 - \left(1 - 2\,\mathrm{d}_{\mathcal{A}}(f)\right)^{k-1}\right) \leq P_k(f) \leq \frac{1}{2}\left(1 - \left(1 - 2\,\mathrm{d}_{\mathcal{A}}(f)\right)^{k+1}\right), \tag{7}$$

where $\mathrm{d}_{\mathcal{A}}(f)$ is the nonlinearity of f. The lower bound above also holds for even k, i.e. for all k we have:

$$\frac{1}{2}\left(1 - \left(1 - 2\,\mathrm{d}_{\mathcal{A}}(f)\right)^{k-1}\right) \leq P_k(f). \tag{8}$$

Proof. In [7, Theorem 3.1], [11, Theorem 2] (and, for $k \leq 3$, in [1]) the following expression for P_k is obtained (we reformulate it for the normalized versions of the definitions of the Walsh transform and nonhomomorphicity):

$$P_k(f) = \frac{1}{2}\left(1 - \sum_{u \in \mathbb{F}_2^n} \left(W(\hat{f})(u)\right)^{k+1}\right), \tag{9}$$

where $\hat{f}(x) = (-1)^{f(x)}$ and $W(\hat{f})$ is the Walsh transform of f. When k is odd (so the exponent $k+1$ is even), all the terms in the sum $S_{k+1} = \sum_{u \in \mathbb{F}_2^n} (W(\hat{f})(u))^{k+1}$ are greater than or equal to zero, so a simple lower bound for this sum is

$$\sum_{u \in \mathbb{F}_2^n} \left(W(\hat{f})(u)\right)^{k+1} \geq \max_{u \in \mathbb{F}_2^n} \left(W(\hat{f})(u)\right)^{k+1} = \left(\max_{u \in \mathbb{F}_2^n} |W(\hat{f})(u)|\right)^{k+1}.$$

Combining the inequality above with $\max_{u \in \mathbb{F}_2^n} |W(\hat{f})(u)| = 1 - 2\,\mathrm{d}_{\mathcal{A}}(f)$ from Equation (4) we obtain the required upper bound.

In order to obtain the lower bound in the statement we need an upper bound on the sum S_{k+1}, which we obtain by a technique similar to the one used in [1]:

$$\sum_{u \in \mathbb{F}_2^n} \left(W(\hat{f})(u)\right)^{k+1} \leq \left(\max_{u \in \mathbb{F}_2^n} |W(\hat{f})(u)|\right)^{k-1} \sum_{u \in \mathbb{F}_2^n} \left(W(\hat{f})(u)\right)^2 = \left(\max_{u \in \mathbb{F}_2^n} |W(\hat{f})(u)|\right)^{k-1},$$

where the last equality uses Parseval's identity (3). Again, using $\max_{u\in\mathbb{F}_2^n} |W(\hat{f})(u)| = 1 - 2\,\mathrm{d}_{\mathcal{A}}(f)$ yields the required lower bound. □

Note that for $k \geq 5$ odd, the bounds in the theorem above are better than the existing bounds (6). We examine the tightness of these bounds. The upper bound for k odd is only attained when exactly one of the Walsh coefficients is nonzero. But this happens if and only if f is affine, which is the trivial case $\mathrm{d}_{\mathcal{A}}(f) = 0$ and $P_k(f) = 0$. However, we found experimentally functions f for which $P_k(f)$ is very close to this upper bound, while $\mathrm{d}_{\mathcal{A}}(f)$ covers many values throughout the interval $(0, 0.5)$. We suspect therefore that the upper bound cannot be improved much.

Let us examine the tightness of the lower bound. For k odd, the lower bound in Theorem 1 is attained by any function f which equals a bent function in m variables for some $2 \leq m \leq n$, m even, for example $f(x_1, x_2, \ldots, x_n) = x_1x_2 + x_3x_4 + \ldots + x_{m-1}x_m$. Such a function has nonlinearity $\mathrm{d}_{\mathcal{A}}(f) = \frac{1}{2}\left(1 - \frac{1}{2^{\frac{m}{2}}}\right)$ and Walsh spectrum with exactly 2^m nonzero entries, all of which are equal to $\pm\frac{1}{2^{\frac{m}{2}}}$. Using (9) we can compute

$$\begin{aligned} P_k(f) &= \frac{1}{2}\left(1 - 2^m\left(\frac{1}{2^{\frac{m}{2}}}\right)^{k+1}\right) \\ &= \frac{1}{2}\left(1 - \left(\frac{1}{2^{\frac{m}{2}}}\right)^{k-1}\right) \\ &= \frac{1}{2}\left(1 - (1 - 2\,\mathrm{d}_{\mathcal{A}}(f))^{k-1}\right) \end{aligned}$$

so the lower bound is attained. Such bent functions have nonlinearity $\frac{1}{4}, \frac{3}{8}, \frac{7}{16}, \ldots$, for $m = 2, 3, 4, \ldots$, respectively. In between these values, the lower bound might not be tight. Indeed for $x < \frac{1}{4}$ a better lower bound was obtained for $k = 3$ in (5) above.

We conjecture that the lower bound (5) can be generalised to arbitrary odd $k \geq 3$ as follows:

Conjecture 2. For any odd $k \geq 3$ we have

$$\begin{aligned} P_k(f) &\geq \frac{1}{2}\max\left(1 - (1-2x)^{k+1} - 2^{k+1}x^k(1-x), 1 - (1-2x)^{k-1}\right) \\ &= \begin{cases} \frac{1}{2}\left(1 - (1-2x)^{k+1} - 2^{k+1}x^k(1-x)\right) & \text{if } x \leq \frac{1}{4} \\ \frac{1}{2}\left(1 - (1-2x)^{k-1}\right) & \text{if } x > \frac{1}{4}, \end{cases} \end{aligned} \tag{10}$$

where $x = \mathrm{d}_{\mathcal{A}}(f)$.

The new bound, if true, would be attained for some functions with nonlinearity in the range $0 < \mathrm{d}_{\mathcal{A}}(f) < \frac{1}{4}$. We can easily find examples for any dimension $n \geq 3$. Take $f(x_1, x_2, x_3, \ldots, x_n) = x_1x_2\ldots x_t$ for some $3 \leq t \leq n$. The Walsh spectrum of such a function contains one entry equal to $1 - \frac{1}{2^{t-1}}$ and $2^t - 1$ entries equal to $\pm\frac{1}{2^{t-1}}$ (with any

further entries being zero). The function has nonlinearity $\mathrm{d}_{\mathcal{A}}(f) = \frac{1}{2^t}$. Using (9) we can compute

$$\begin{aligned} P_k(f) &= \frac{1}{2}\left(1 - \left(1 - \frac{1}{2^{t-1}}\right)^{k+1} - (2^t - 1)\left(\frac{1}{2^{t-1}}\right)^{k+1}\right) \\ &= \frac{1}{2}\left(1 - \frac{(2^{t-1}-1)^{k+1} + (2^t - 1)}{2^{(t-1)(k+1)}}\right). \end{aligned}$$

On the other hand, computing the lower bound by substituting $x = \frac{1}{2^t}$ in (10) we obtain

$$\begin{aligned} P_k(f) &\geq \frac{1}{2}\left(1 - \left(1 - \frac{1}{2^{t-1}}\right)^{k+1} - 2^{k+1}\frac{1}{2^{tk}}\left(1 - \frac{1}{2^t}\right)\right) \\ &= \frac{1}{2}\left(1 - \frac{(2^{t-1}-1)^{k+1} + (2^t - 1)}{2^{(t-1)(k+1)}}\right) \end{aligned}$$

so the lower bound is attained. Again, this shows that this conjectured lower bound is attained at non-linearity equal to $\frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \ldots$ but in between these values it might not be tight.

4 Affinity tests using linearity tests and bounds on the probability of failure

We propose a new affinity test, based on any linearity test. It uses a simple observation: a function f is affine if and only if either f or $f+1$ is linear. The probability of f failing this affinity test is the minimum between the probability of f failing the linearity test, and the probability of $f+1$ failing the linearity test. In [11] it is shown that for k even (when $P_k(f) = 0$ indicates that f is linear), f is affine if and only if $P_k(f) \in \{0, 1\}$. However, there are no results about what happens when $P_k(f) \notin \{0, 1\}$, in terms of the relationship of this probability to nonlinearity.

If we use the BLR linearity test or, more generally, the k-th order nonhomomorphicity test for k even, note that $f + 1$ passes the test for some given arguments if and only if f fails the test for those arguments; so we do not need to run the test for both f and for $f + 1$, but only for one of them. We still need only $k + 1$ queries per test rather than $2(k+1)$. Denoting by $\overline{P}_k(f)$ the probability of failure of the proposed test for affine functions we have

$$\overline{P}_k(f) = \min(P_k(f), P_k(f+1)) = \min(P_k(f), 1 - P_k(f)).$$

In Bellare et al. [1] lower and upper bounds are given for $\mathrm{P}_2(f)$ in terms of $\mathrm{d}_{\mathcal{L}}(f)$. Namely it is proven that

$$\mathrm{Lower}_2(\mathrm{d}_{\mathcal{L}}(f)) \leq \mathrm{P}_2(f) \leq \mathrm{Upper}_2(\mathrm{d}_{\mathcal{L}}(f))), \tag{11}$$

where $\text{Lower}_2, \text{Upper}_2 : [0, \frac{1}{2}] \to \mathbb{R}$ are defined as

$$\text{Lower}_2(x) = \begin{cases} 3x - 6x^2 & \text{if } x \le \frac{1}{4} \\ \max\left(3x - 6x^2, \frac{45}{128}, x\right) & \text{if } x > \frac{1}{4} \end{cases} \tag{12}$$

and $\text{Upper}_2(0) = 0$ and for $x > 0$

$$\text{Upper}_2(x) = 3x - 6x^2 + 2^{2\lfloor \log_2 x \rfloor + 2} + 12\left(x - 2^{\lfloor \log_2 x \rfloor}\right)^2. \tag{13}$$

We now prove bounds for $\overline{\text{P}}_2(f)$ in terms of $\text{d}_{\mathcal{A}}(f)$, the distance to the closest *affine* function, which is the natural parameter to consider when testing if a function is affine. Note that in the following theorem, although the bounds look similar to the bounds in (11) above, there is a subtle and important difference: the bounds are now a function of $\text{d}_{\mathcal{A}}(f)$, the distance to the closest *affine* function, whereas in (11) the bounds are expressed in terms of $\text{d}_{\mathcal{L}}(f)$, the distance to the closest *linear* function.

Theorem 3. *The probability of failure of the proposed affinity test,* $\overline{\text{P}}_2(f) = \min(\text{P}_2(f), 1 - \text{P}_2(f))$ *satisfies the following inequalities,*

$$\text{Lower}_2\left(\text{d}_{\mathcal{A}}(f)\right) \le \overline{\text{P}}_2(f) \le \min\left(\frac{1}{2}, \text{Upper}_2(\text{d}_{\mathcal{A}}(f))\right), \tag{14}$$

where $\text{d}_{\mathcal{A}}(f)$ *is the nonlinearity of* f *and* $\text{Lower}_2(x)$ *and* $\text{Upper}_2(x)$ *are as defined above in* (12) *and* (13)*.*

Proof. We know that $\text{d}_{\mathcal{A}}(f) = \min(\text{d}_{\mathcal{L}}(f), \text{d}_{\mathcal{L}}(f+1))$. We can assume, without loss of generality, that $\text{d}_{\mathcal{L}}(f) \le \text{d}_{\mathcal{L}}(f+1)$ (otherwise, we can just replace f by $f+1$, and $\overline{\text{P}}_2(f)$ is unchanged). Therefore $\text{d}_{\mathcal{A}}(f) = \text{d}_{\mathcal{L}}(f)$.

First let us examine the function $\text{Upper}_2(x)$ more closely. If $\frac{1}{4} \le x < \frac{1}{2}$ then $\lfloor \log_2 x \rfloor = -2$ so a simple computation shows that $\text{Upper}_2(x) = 6x^2 - 3x + 1$ in this case. If $\frac{1}{8} \le x < \frac{1}{4}$ then $\lfloor \log_2 x \rfloor = -3$ so a simple computation shows that $\text{Upper}_2(x) = 6x^2 + \frac{1}{4}$ in this case. In particular, note that the function $\text{Upper}_2(x)$ crosses the line $y = \frac{1}{2}$ at $x = \frac{1}{2\sqrt{6}}$ (namely $\text{Upper}_2(x) \ge \frac{1}{2}$ if and only if $x \ge \frac{1}{2\sqrt{6}}$) and $\frac{1}{8} \le \frac{1}{2\sqrt{6}} < \frac{1}{4}$. Also, one can check that the function $\text{Upper}_2(x)$ is monotonically increasing on the domain $\left[0, \frac{1}{2}\right]$. (It is continuous, and the derivative exists at all points except those of the form $x = \frac{1}{2^m}$ for some integer $m \ge 1$. The derivative is greater than zero at all points where it exists.)

For the upper bound, from (11) we have

$$\begin{aligned} \text{P}_2(f) &\le \text{Upper}_2\left(\text{d}_{\mathcal{L}}(f)\right) \\ 1 - \text{P}_2(f) &= \text{P}_2(f+1) \le \text{Upper}_2\left(\text{d}_{\mathcal{L}}(f+1)\right). \end{aligned}$$

Therefore, using the fact that Upper_2 is monotonic and the assumption $\text{d}_{\mathcal{L}}(f) \le \text{d}_{\mathcal{L}}(f+1)$ we obtain

$$\begin{aligned} \overline{\text{P}}_2(f) &= \min(\text{P}_2(f), 1 - \text{P}_2(f)) \\ &\le \min(\text{Upper}_2(\text{d}_{\mathcal{L}}(f)), \text{Upper}_2(\text{d}_{\mathcal{L}}(f+1))) \\ &= \text{Upper}_2(\text{d}_{\mathcal{L}}(f)) = \text{Upper}_2(\text{d}_{\mathcal{A}}(f)). \end{aligned}$$

The bound $\overline{\mathrm{P}}_2(f) \leq \frac{1}{2}$ is immediate from the definition of $\overline{\mathrm{P}}_2(f)$.

Now let us deal with the lower bound. If $\mathrm{P}_2(f) \leq 1-\mathrm{P}_2(f)$ (in other words $\mathrm{P}_2(f) \leq \frac{1}{2}$), then $\overline{\mathrm{P}}_2(f) = \mathrm{P}_2(f) \geq \mathrm{Lower}_2(\mathrm{d}_{\mathcal{L}}(f)) = \mathrm{Lower}_2(\mathrm{d}_{\mathcal{A}}(f))$ and we are done. Let us assume $\mathrm{P}_2(f) > 1 - \mathrm{P}_2(f)$ i.e. $\mathrm{P}_2(f) > \frac{1}{2}$. From the behaviour of $\mathrm{Upper}_2(x)$ discussed above, we see that this can only happen when $\mathrm{d}_{\mathcal{L}}(f) \geq \frac{1}{2\sqrt{6}}$. We have to prove that in this case $1 - \mathrm{P}_2(f) \geq \mathrm{Lower}_2(\mathrm{d}_{\mathcal{L}}(f))$.

Let us first consider the case $\frac{1}{2\sqrt{6}} \leq \mathrm{d}_{\mathcal{L}}(f) \leq \frac{1}{4}$. We have

$$\mathrm{P}_2(f) \leq \mathrm{Upper}_2\left(\mathrm{d}_{\mathcal{L}}(f)\right) = 6\left(\mathrm{d}_{\mathcal{L}}(f)\right)^2 + \frac{1}{4},$$

therefore

$$1-\mathrm{P}_2(f) \geq 1-6\left(\mathrm{d}_{\mathcal{L}}(f)\right)^2 - \frac{1}{4} = \frac{3}{4} - 6\left(\mathrm{d}_{\mathcal{L}}(f)\right)^2 \geq 3\,\mathrm{d}_{\mathcal{L}}(f) - 6\left(\mathrm{d}_{\mathcal{L}}(f)\right)^2 = \mathrm{Lower}_2\left(\mathrm{d}_{\mathcal{L}}(f)\right),$$

where the last inequality uses the fact that $\mathrm{d}_{\mathcal{L}}(f) \leq \frac{1}{4}$.

Next assume that $\frac{1}{4} < \mathrm{d}_{\mathcal{A}}(f)$. When $x \in \left[\frac{1}{4}, \frac{1}{2}\right]$ the function $\mathrm{Lower}_2(x)$ behaves as follows:

$$\mathrm{Lower}_2(x) = \begin{cases} 3x - 6x^2 & \text{if } \frac{1}{4} \leq x < \frac{5}{16} \\ \frac{45}{128} & \text{if } \frac{5}{16} \leq x \leq \frac{45}{128} \\ x & \text{if } \frac{45}{128} \leq x \leq \frac{1}{2}, \end{cases}$$

(observe that $\frac{3}{16}, \frac{5}{16}$ are the two solutions of the equation $3x - 6x^2 = \frac{45}{128}$).

Consider first the subcase $\frac{1}{4} \leq \mathrm{d}_{\mathcal{A}}(f) < \frac{5}{16}$. We have:

$$\mathrm{P}_2(f) \leq \mathrm{Upper}_2\left(\mathrm{d}_{\mathcal{L}}(f)\right)$$

and therefore using the fact that $\mathrm{Upper}_2(x) = 6x^2 - 3x + 1$ when $x \geq \frac{1}{4}$

$$1 - \mathrm{P}_2(f) \geq 1 - \mathrm{Upper}_2\left(\mathrm{d}_{\mathcal{L}}(f)\right) = 3\,\mathrm{d}_{\mathcal{L}}(f) - 6\left(\mathrm{d}_{\mathcal{L}}(f)\right)^2 = \mathrm{Lower}_2\left(\mathrm{d}_{\mathcal{L}}(f)\right).$$

Finally, let us consider the subcase $\mathrm{d}_{\mathcal{A}}(f) \geq \frac{5}{16}$. We have

$$1 - \mathrm{P}_2(f) = \mathrm{P}_2(f+1) \geq \mathrm{Lower}_2\left(\mathrm{d}_{\mathcal{L}}(f+1)\right) \geq \mathrm{Lower}_2\left(\mathrm{d}_{\mathcal{L}}(f)\right)$$

with the last inequality based on the fact that $\frac{5}{16} < \mathrm{d}_{\mathcal{L}}(f) \leq \mathrm{d}_{\mathcal{L}}(f+1)$ and $\mathrm{Lower}_2(x)$ is monotonic when the argument is above $\frac{5}{16}$. □

Further refinements of the lower bound for the BLR linearity test are given in [8]. Their effect on the bounds for the affinity test proposed here will be investigated as further work.

5 Estimating nonlinearity

The tests above for affine functions can be used to estimate the nonlinearity of a Boolean function. The probability of failing a test can be estimated by running the test several times and using statistical methods such as the binomial proportion confidence interval. The bounds will then allow to give an interval for the value of the nonlinearity as per (2) and (1). We will examine each test in turn.

We first look at the test based on the BLR test, and we refer to the graph in the Appendix, displaying the lower and upper bound described in Theorem 3. Thus, for values of $\overline{\mathrm{P}}_2(f) < \frac{45}{128} = 0.3515625$, then $\mathrm{d}_{\mathcal{A}}(f)$ can be estimated with good precision as being in the interval

$$\mathrm{d}_{\mathcal{A}}(f) \in \left[{\mathrm{Upper}_2}^{-1}(\overline{\mathrm{P}}_2(f)), {\mathrm{Lower}_2}^{-1}(\overline{\mathrm{P}}_2(f))\right].$$

The length of this interval increases with $\overline{\mathrm{P}}_2(f)$ to a length of approximately 0.058. For $\frac{45}{128} \le \overline{\mathrm{P}}_2(f) < \frac{1}{4}$, ${\mathrm{Lower}_2}^{-1}(\overline{\mathrm{P}}_2(f)) = \{\alpha_1, \alpha_2, \overline{\mathrm{P}}_2(f)\}$ where $\alpha_1 \le \alpha_2$ are the two roots of the equation $3x - 6x^2 = \overline{\mathrm{P}}_2(f)$. We obtain two disjoint intervals where $\mathrm{d}_{\mathcal{A}}(f)$ might belong to:

$$\mathrm{d}_{\mathcal{A}}(f) \in \left[{\mathrm{Upper}_2}^{-1}(\overline{\mathrm{P}}_2(f)), \alpha_1\right] \cup \left[\alpha_2, \overline{\mathrm{P}}_2(f)\right].$$

Finally, for $\overline{\mathrm{P}}_2(f) \ge \frac{1}{4}$, the interval for $\mathrm{d}_{\mathcal{A}}(f)$ is $\left[{\mathrm{Upper}_2}^{-1}(\overline{\mathrm{P}}_2(f)), \overline{\mathrm{P}}_2(f)\right]$. The estimate for $\mathrm{d}_{\mathcal{A}}(f)$ becomes less and less precise as $\overline{\mathrm{P}}_2(f)$ increases (the interval length increases). As $\overline{\mathrm{P}}_2(f)$ reaches $\frac{1}{2}$ we obtain $\mathrm{d}_{\mathcal{A}}(f) \in \left[\frac{1}{2\sqrt{6}}, \frac{1}{2}\right)$, an interval of length approximately 0.295.

Next we look at the test $f(x_1 + \cdots + x_k) + f(x_1) + \cdots + f(x_k) = 0$ with k odd. For $k = 3$, looking at the graph in the Appendix of the lower bound Lower_3 given in (5) and the upper bound Upper_3 given in Theorem 1, for values of $\mathrm{P}_3(f) < 0.375$, the value of $\mathrm{d}_{\mathcal{A}}(f)$ can be estimated with good precision as being in the interval

$$\mathrm{d}_{\mathcal{A}}(f) \in \left[{\mathrm{Upper}_3}^{-1}(\mathrm{P}_3(f)), {\mathrm{Lower}_3}^{-1}(\mathrm{P}_3(f))\right].$$

The length of this interval increases with $\mathrm{P}_3(f)$ to a length of approximately 0.03. When $0.375 \le \mathrm{P}_3(f) < 0.3849$ the function Lower_3 is not invertible (it has 3 values in the preimage of any point in this interval) and the possible values of $\mathrm{d}_{\mathcal{A}}(f)$ are in two disjoint intervals. For example, for $\mathrm{P}_3(f) = 0.38$ we have $\mathrm{d}_{\mathcal{A}}(f) \in [0.15, 0.186] \cup [0.238, 0.256]$. Finally, for $0.3849 \le \mathrm{P}_3(f) \le 0.5$ the estimate is $\mathrm{d}_{\mathcal{A}}(f) \in [\frac{1}{2}(1 - \sqrt[4]{1 - 2\,\mathrm{P}_3(f)}), \frac{1}{2}(1 - \sqrt{1 - 2\,\mathrm{P}_3(f)})]$ which is a larger interval, peaking around $\mathrm{P}_3(f) = 0.469$ where we have $\mathrm{d}_{\mathcal{A}}(f) \in [0.251, 0.376]$, with an interval of size 0.125.

Finally we look at the test $f(x_1 + \cdots + x_k) + f(x_1) + \cdots + f(x_k) = 0$ with k odd, $k \ge 5$. Using the bounds in Theorem 1 we have that, once $P_k(f)$ has been estimated by statistical methods, $\mathrm{d}_{\mathcal{A}}(f)$ can be estimated as

$$\mathrm{d}_{\mathcal{A}}(f) \in \left[\frac{1}{2}\left(1 - \sqrt[k+1]{1 - 2P_k(f)}\right), \frac{1}{2}\left(1 - \sqrt[k-1]{1 - 2P_k(f)}\right)\right]. \tag{15}$$

Note that the less tight bounds (6) used in [11] would give the considerably less accurate estimate

$$\mathrm{d}_{\mathcal{A}}(f) \in \left[0, \frac{1}{2}\left(1 - \sqrt[k+1]{\frac{1-2P_k(f)}{2^n}}\right)\right].$$

The length of the interval produced by our estimate (15) is

$$\frac{1}{2}\left(\sqrt[k+1]{1-2P_k(f)} - \sqrt[k-1]{1-2P_k(f)}\right).$$

This quantity has a unimodal behavior: the length increases as a function of $P_k(f)$, from 0 (for $P_k(f) = 0$), peaks at a value of

$$\frac{1}{2}\left(\left(\frac{k-1}{k+1}\right)^{\frac{k-1}{2}} - \left(\frac{k-1}{k+1}\right)^{\frac{k+1}{2}}\right),$$

achieved when

$$P_k(f) = \frac{1}{2}\left(1 - \left(\frac{k-1}{k+1}\right)^{\frac{k^2-1}{2}}\right),$$

and then decreases again to 0 as $P_k(f)$ reaches 0.5. For example for $k = 5$ the length of the interval peaks at a value of 0.0741 (achieved when $P_k(f) = 0.496$). For $k = 7$ the previous displayed length peaks to a value of 0.05273 achieved at $P_k(f) = 0.4995$. The maximum length of the interval is achieved when $P_k(f)$ is quite close to 0.5; the larger the value of k, the smaller the maximum length of the interval, i.e. the more precisely we can estimate the nonlinearity.

To conclude this section, we note that all tests are quite accurate in estimating nonlinearity when the probability of failing the test is small (and consequently the nonlinearity is small), but the accuracy decreases as the probability of failing the test increases. Throughout the range, the BLR test is less accurate than the k-nonhomomorphicity test ($k > 2$) for estimating the nonlinearity. The accuracy of the k-order nonhomomorphicity test improves as k increases.

Acknowledgments. The authors are grateful to the reviewers for extensive and helpful comments and suggestions which have highly improved the manuscript.

References

[1] M. Bellare, D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan. Linearity testing in characteristic two. *IEEE Trans. Inf. Theory*, 42(6):1781–1795, 1996.

[2] D. Bera, S. Maitra, D. Roy, and P. Stănică. Limitation of the BLR testing in estimating nonlinearity. In *Workshop on Coding and Cryptography*, Rennes, France, 2019, Paper #50.

[3] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. Syst. Sci.*, 47(3): 549–595, 1993.

[4] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

[5] I. Dinur and A. Shamir. Cube attacks on tweakable black box polynomials. *Advances in Cryptology – EUROCRYPT* 2009, pp. 278–299, LNCS 5479. Springer, Berlin, Heidelberg.

[6] I. Dinur and A. Shamir. Applying cube attacks to stream ciphers in realistic scenarios. *Cryptography and Communications*, 4(3-4):217–232, 2012.

[7] A. Doğanaksoy, S. Sağdiçoğlu, Z. Saygi, and M. Uğuz, A note on linearity and homomorphicity. In J-F. Michon, P. Valarcher, and J.-B. Yunès, editors, *Boolean Functions: Cryptography and Applications*, pages 280–295, 2006.

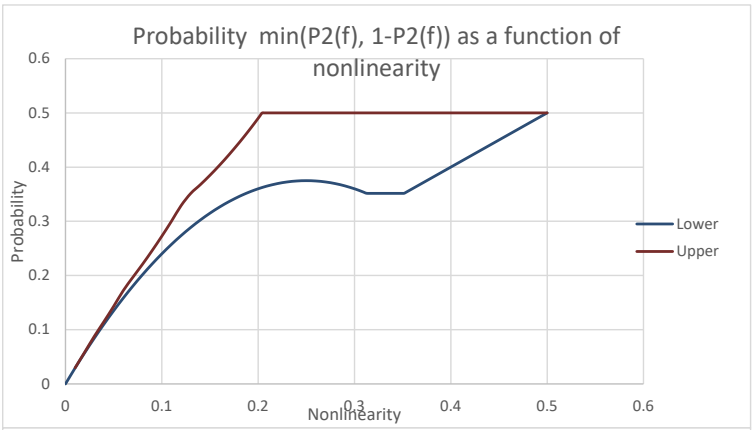
[8] T. Kaufman, S. Litsyn, and N. Xie. Breaking the ϵ-soundness bound of the linearity test over GF(2). *SIAM J. Computing*, 39(5):1988–2003, 2010.

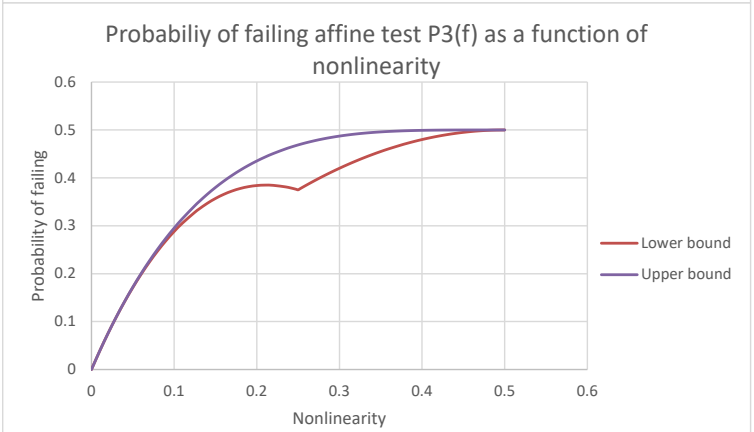
[9] M. Vielhaber. Breaking ONE.FIVIUM by AIDA an algebraic IV differential attack. Cryptology ePrint Archive, Report 2007/413, 2007. http://eprint.iacr.org/.

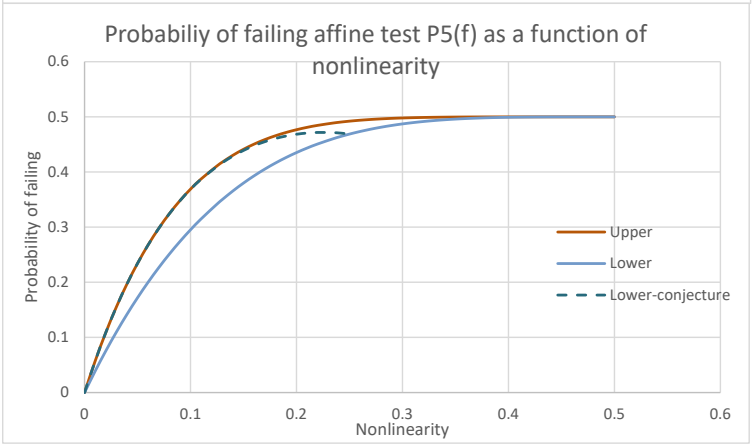
[10] R. Winter, A. Sălăgean, and R. C. W. Phan. Comparison of cube attacks over different vector spaces. In Jens Groth, editor, 15*th IMA International Conference on Cryptography and Coding, IMACC*, LNCS 9496, pp. 225–238. Springer, 2015.

[11] X.-M. Zhang and Y. Zheng. The nonhomomorphicity of Boolean functions. In Stafford Tavares and Henk Meijer, editors, *Selected Areas in Cryptography*, pp. 280–295. Springer, 1999.

Appendix


Probability min(P2(f), 1-P2(f)) as a function of nonlinearity
Probability
Nonlinearity
Lower
Upper


Probabiliy of failing affine test P3(f) as a function of nonlinearity
Probability of failing
Nonlinearity
Lower bound
Upper bound


Probabiliy of failing affine test P5(f) as a function of nonlinearity
Probability of failing
Nonlinearity
Upper
Lower
Lower-conjecture