



Counting Boolean functions with faster points

Ana Sălăgean¹  · Ferruh Özbudak²

Received: 29 May 2019 / Revised: 28 January 2020 / Accepted: 5 February 2020
© The Author(s) 2020

Abstract

Duan and Lai introduced the notion of “fast point” for a Boolean function f as being a direction a so that the algebraic degree of the derivative of f in direction a is strictly lower than the expected $\deg(f) - 1$. Their study was motivated by the fact that the existence of fast points makes many cryptographic differential attacks (such as the cube and AIDA attack) more efficient. The number of functions with fast points was determined by Duan et al. in some special cases and by Sălăgean and Mandache-Sălăgean in the general case. We generalise the notion of fast point, defining a fast point of order ℓ as being a fast point a so that the degree of the derivative of f in direction a is lower by at least ℓ than the expected degree. We determine an explicit formula for the number of functions of degree d in n variables which have fast points of order ℓ . Furthermore, we determine the number of functions of degree d in n variables which have a given number of fast points of order ℓ , and also the number of functions which have a given profile in terms of the number of fast points of each order. We apply our results to compute the probability of a function to have fast points of order ℓ . We also compute the number of functions which admit linear structures (i.e. their derivative in a certain direction is constant); such functions have a long history of being used in the analysis of symmetric ciphers.

Keywords Boolean functions · Differential attacks · Linear structures

Mathematics Subject Classification 94A60 · 11T55

This is one of several papers published in *Designs, Codes and Cryptography* comprising the “Special Issue on Coding and Cryptography 2019”.

✉ Ana Sălăgean
a.m.salagean@lboro.ac.uk
Ferruh Özbudak
ozbudak@metu.edu.tr

¹ Department of Computer Science, Loughborough University, Loughborough, UK

² Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

1 Introduction

Boolean functions used in cryptography are usually required to resist a range of attacks. They need to have a sufficiently high algebraic degree (i.e. the degree of the function written in its algebraic normal form) in order to resist algebraic attacks. Differential attacks on cryptographic functions typically exploit properties of the discrete derivative. The discrete derivative of a function f in the direction a is defined as $D_a f(x) = f(x + a) - f(x)$. The derivatives should also have a high degree; the highest that can be achieved is one less than the degree of the original function, i.e. $\deg(D_a f) \leq \deg(f) - 1$. Higher order derivatives of order k are obtained by differentiating k times in several directions. The higher order derivatives should also have a sufficiently high degree (the maximum possible being $\deg(f) - k$). For example, the cube attack of Dinur and Shamir [5] and the AIDA attack of Vielhaber [14], as well as further variants of these attacks, exploit the situation where a higher order derivative of the function has a very low degree (degree 1 in the original AIDA and cube attacks, degree 1 or 2 in [1] and [8] for example; cube testers introduced in [2] test for several non-randomness properties, one of which being low degree). Computing a higher order derivative of order k is computationally expensive as k increases (2^k complexity) so the attacks work particularly well when the degree drops quicker than expected.

Motivated by these applications, Duan and Lai [6] introduced the notion of “fast point” for a cryptographic function: a is a fast point for a function f if the degree of $D_a f$ drops more than expected, i.e. the degree is strictly lower than $\deg(f) - 1$. The fast points of a function f form a linear space. Duan et al. [7] started computing the number of functions that admit fast points; explicit formulae were obtained for small degrees and very large degrees (close to the number of variables), and exhaustive search results were obtained for small numbers of variables.

Sălăgean and Mandache-Sălăgean [13] obtained a recurrence relation as well as an explicit formula for the number of functions that admit fast points, for any number of variables n and any degree d . This sequence of numbers (triangular sequence indexed by n and d for $1 \leq d \leq n$) is given as sequence A316554 in OEIS (Online Encyclopedia of Integer Sequences, [12]) and it solves the cases left open by Duan et al. in [7]. Moreover, the counting is refined to functions of degree d in n variables which admit a particular number of fast points, i.e. their space of fast points has a particular dimension.

In this paper we define “faster points” i.e. points where the degree of the derivative drops by at least 2 more than expected. More generally, a fast point of order ℓ for a function f will be a point where the degree of $D_a f$ is at most $\deg(f) - 1 - \ell$, i.e. it dropped ℓ more than expected. The fast points of order ℓ of a function f form a linear space. The dimensions of these spaces are affine invariants, i.e. they are invariant to invertible affine changes of coordinates.

In Sect. 3 we will count the number of functions of degree d in n variables which have a given space U as their space of fast points of order ℓ . This number does not depend on the space itself, only on its dimension, so this allows us to count, for each fixed k , the number of functions which have exactly 2^k fast points of order ℓ ; also the number of functions which have no fast points of order ℓ . For all these numbers we give both recurrence relations and explicit formulae, see Theorem 2 for fast points of order 2 and Theorem 3 for arbitrary order. The proofs use some techniques similar to the ones in [13], but also some different techniques, particularly a version of the inversion formulae of Carlitz [3], see Lemma 2.

As an application of these counting results, in Sect. 4 we determine the number of functions which have linear structures. The notion of linear structure was introduced by Chaum and

Evertse in 1985 in [4] and has since been used widely in the analysis of cryptographic primitives. An element a is a *linear structure* for a function f if $D_a f$ is a constant function. With our definition, a linear structure for f is a fast point of order $\deg(f) - 1$, so we can apply our results directly to compute the number of functions which have linear structures for each degree d and n variables.

A second application is to estimate the probability that a function picked uniformly at random has fast points of order ℓ ; also the probability that a function has fast points of order ℓ when we pick it from among the functions which do have fast points of order $\ell - 1$. All these probabilities are extremely small (see Proposition 1).

We further refine our counting results in Sect. 5. For each fixed sequence of spaces $U_1 \supseteq U_2 \supseteq \dots \supseteq U_\ell$ we count the number of functions which have exactly those U_i as their space of fast points of order i . Also, for $k_1 \geq k_2 \geq \dots \geq k_\ell$ we count the functions whose space of fast points of order i has dimension k_i , for $i = 1, \dots, \ell$. The new aspect here compared to the results in Sect. 3 is that we also need to count functions which *do not* have any fast points in a particular subspace. For all these numbers we give explicit formulae, see Theorem 4.

Note that although we count the number of functions for each set of given values of these affine invariants, this is different from counting the number of equivalence classes and the size of each class under the equivalence given by affine invertible changes of coordinates. For the latter, Hou [9] and Langevin and Leander [11] obtained results for up to 8 variables by a combination of theoretical results and computer search, and combining several invariants to discriminate each class. What we compute here is the sum of the cardinalities of those classes which share a particular value of the invariant defined as the dimensions of the space of fast points of each order (and there are several classes with the same value of this invariant).

2 Preliminaries

We denote by \mathbb{F}_2 the binary field. A Boolean function f with n -bits input and one bit output can be viewed as a function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Any such function can be represented in algebraic form as a polynomial function in n variables, of degree at most one in each variable. (More precisely, because $x^2 = x$ when $x \in \mathbb{F}_2$, each function corresponds to an element in $\mathbb{F}_2[x_1, \dots, x_n]/\langle x_1^2 + x_1, \dots, x_n^2 + x_n \rangle$; we identify each coset with its unique representative multivariate polynomial which has degree at most one in each variable.) The total degree of this multivariate polynomial is called the algebraic degree of the function f . In this paper we will call the algebraic degree of f simply the degree of f , denoted $\deg(f)$, with the usual convention that the degree of the zero function is $-\infty$. We will denote by $\text{BF}(n)$ the set of Boolean functions in n variables, and by $\text{BF}(n, d)$ the set of Boolean functions in n variables of degree exactly d , where $0 \leq d \leq n$.

Let $f \in \text{BF}(n, d)$ and $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, where $\mathbf{0}$ denotes the all-zero vector. The *derivative* $D_a f$ of f in direction a is defined as the Boolean function in n variables $x \mapsto f(x + a) - f(x)$. The degree of $D_a f$ is lower than or equal to $d - 1$ (see [10]), i.e. differentiation decreases the degree of the function by at least 1. Vectors a for which the degree of $D_a f$ is strictly lower than $d - 1$ (i.e. the degree drops more than expected) are called “fast points” of f (see [6]). The set of fast points of f (including, by convention, $\mathbf{0}$ as a trivial fast point) is a linear subspace of \mathbb{F}_2^n of dimension at most $n - d$ (see [6]).

Note that if f has degree d , then only its monomials of degree d matter when determining whether the degree of $D_a f$ is equal to $d - 1$ or strictly lower, and therefore determining whether a is a fast point. In other words, $a \in \mathbb{F}_2^n$ is a fast point of f if and only if a is a fast

point of $f + g$, where g is an arbitrary Boolean function in n variables of degree at most $d - 1$. Hence for counting Boolean functions having fast points, it is natural to define the following equivalence on $\text{BF}(n)$: for $f_1, f_2 \in \text{BF}(n)$

$$f_1 \stackrel{(i)}{\sim} f_2 \iff \deg(f_1 - f_2) \leq i.$$

Then $[f]^{(i)}$ denotes the equivalence class of f with respect to the $\stackrel{(i)}{\sim}$ equivalence relation.

For deciding whether a function f of degree d has fast points, it suffices to consider f up to the equivalence $\stackrel{(d-1)}{\sim}$.

Next we formally define “faster points”.

Definition 1 Let $f \in B(n, d)$ and $1 \leq \ell \leq d$. An element $a \in \mathbb{F}_2^n, a \neq \mathbf{0}$ is called a *fast point of order ℓ* for f if $\deg(D_a f) \leq d - 1 - \ell$. The set of fast points of order ℓ of f (including, by convention, $\mathbf{0}$) is denoted

$$\text{FP}^{(\ell)}(f) = \{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \deg(D_a f) \leq d - 1 - \ell\} \cup \{\mathbf{0}\}. \quad (1)$$

Note the usual fast points are fast points of order 1. If $a_1, a_2 \in \text{FP}^{(\ell)}(f)$, then

$$\begin{aligned} D_{a_1+a_2} f(x) &= f(x + a_1 + a_2) - f(x) \\ &= f(x + a_1 + a_2) - f(x + a_1) + f(x + a_1) - f(x) \\ &= D_{a_2} f(x + a_1) + D_{a_1} f(x). \end{aligned}$$

Hence $\deg(D_{a_1+a_2} f) \leq \max\{\deg(D_{a_1} f), \deg(D_{a_2} f)\}$. This proves that $\text{FP}^{(\ell)}(f)$ is a linear subspace of \mathbb{F}_2^n . The dimension of this space is at most $n - d$, since a fast point of order ℓ is also a fast point of order $\ell - 1$ and $\dim(\text{FP}^{(1)}(f)) \leq n - d$. We have a filtration of linear subspaces:

$$\mathbb{F}_2^n \supseteq \text{FP}^{(1)}(f) \supseteq \text{FP}^{(2)}(f) \supseteq \dots \supseteq \text{FP}^{(d-1)}(f) \supseteq \text{FP}^{(d)}(f) \supseteq \{\mathbf{0}\}.$$

When determining whether a function f of degree d has fast points of order ℓ only the monomials of degree $d, d - 1, \dots, d - \ell + 1$ matter, as they are the only ones that can produce polynomials of degree strictly above $d - 1 - \ell$ after differentiation; so we only need to consider the function f up to the equivalence $\stackrel{(d-\ell)}{\sim}$. The set of functions (up to the suitable equivalence) which have their space of fast points of order ℓ equal to a given subspace $U \subseteq \mathbb{F}_2^n$ will be denoted:

$$\text{F}^{(\ell)}(n, d; U) = \{[f]^{(d-\ell)} : f \in \text{BF}(n, d) \text{ and } \text{FP}^{(\ell)}(f) = U\}.$$

The set of functions (up to the suitable equivalence) for which the space of fast points of order ℓ has a given dimension k will be denoted:

$$\text{F}^{(\ell)}(n, d; k) = \{[f]^{(d-\ell)} : f \in \text{BF}(n, d) \text{ and } \dim(\text{FP}^{(\ell)}(f)) = k\}.$$

In particular, $\text{F}^{(\ell)}(n, d; 0)$ is the set of functions (up to the suitable equivalence) which have no fast points of order ℓ .

For integers $0 \leq k \leq n$ the Gaussian binomial coefficients (or q -binomial coefficients) are defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}. \quad (2)$$

Recall that the number of k dimensional \mathbb{F}_q -linear subspaces of \mathbb{F}_q^n (when q is a power of a prime) is $\begin{bmatrix} n \\ k \end{bmatrix}_q$. We will mostly use these Gaussian binomial coefficients for $q = 2$, and in this case we will omit the index and simply denote $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix}_2$.

For the cardinality of $F^{(1)}(n, d; k)$ a recurrence relation as well as an explicit formula were computed by Sălăgean and Mandache-Sălăgean, [13]. The number of functions of degree d in n variables which have fast points was also computed (see sequence A316554 in OEIS, [12]). We recall the explicit formulae:

Theorem 1 ([13, Theorem 6, Corollary 3]) *Let integers n, d, k be such that $1 \leq d \leq n$ and $0 \leq k \leq n - d$. The number of functions of degree d in n variables which have fast points is:*

$$\sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \left(2^{\binom{n-i}{d}} - 1 \right).$$

We have

$$|F^{(1)}(n, d; k)| = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{i=0}^{n-k-d} (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n-k \\ i \end{bmatrix} \left(2^{\binom{n-k-i}{d}} - 1 \right).$$

For $1 \leq i \leq n$ let $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{F}_2^n$ be the vector which has 1 in its i -th position and zeroes elsewhere. The set $\{e_1, \dots, e_n\}$ forms the standard basis (canonical basis) of \mathbb{F}_2^n over \mathbb{F}_2 .

Most properties we are interested in are invariant to linear (or affine) changes of variables (changes of coordinates). Recall that two functions $f_1, f_2 : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ are called *affine equivalent* if there is an invertible affine map $\varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ such that $f_1 = f_2 \circ \varphi$. Any function P (or a relation) defined over the set of Boolean function is called an *affine invariant* if $P(f_1) = P(f_2)$ for any two affine equivalent functions f_1, f_2 . A few useful facts are collected below:

Lemma 1 *Let $f, f_1, f_2 : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ and $a \in \mathbb{F}_2^n$. Let $\varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be an invertible linear (or affine) map.*

- (i) *The degree of a function is an affine invariant, i.e. $\deg(f) = \deg(f \circ \varphi)$.*
- (ii) *$D_a(f \circ \varphi) = (D_{\varphi(a)}f) \circ \varphi$.*
- (iii) *The property of a function having fast points of order ℓ is an affine invariant. More precisely, a is a fast point of order ℓ for f iff $\varphi^{-1}(a)$ is a fast point of order ℓ for $f \circ \varphi$.*
- (iv) *e_i is a fast point of order ℓ for f iff x_i does not appear in any of the monomials of degree $d, d-1, \dots, d-\ell+1$ of f .*
- (v) *$f_1 \stackrel{(i)}{\sim} f_2$ iff $f_1 \circ \varphi \stackrel{(i)}{\sim} f_2 \circ \varphi$.*

3 Counting faster points

We will make extensive use of the following inversion formula, which is a variant of the result of Carlitz [3]:

Lemma 2 *Let $S, T : \mathbb{N} \rightarrow \mathbb{C}$ be functions. Then*

$$S(n) = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q T(k) \text{ for all } n \geq 0 \quad (3)$$

if and only if

$$T(n) = \sum_{k=0}^n (-1)^k q^{\frac{k(k-1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q S(n-k) \text{ for all } n \geq 0. \quad (4)$$

Proof We recall [3, Theorem 2]. Let (a_i) and (b_i) be sequences of complex numbers, and q a complex number such that $a_i + q^{-k}b_i \neq 0$ for all $i \geq 1$ and $k \geq 0$. Put $\psi(k, n, q) = \prod_{i=1}^n (a_i + q^{-k}b_i)$. The system of equations

$$f(n) = \sum_{k=0}^n (-1)^k q^{\frac{k(k-1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q \psi(k, n, q) g(k) \text{ for all } n \geq 0$$

is equivalent to the system

$$g(n) = \sum_{k=0}^n (-1)^k q^{\frac{k(k+1)}{2} - kn} \begin{bmatrix} n \\ k \end{bmatrix}_q (a_{k+1} + q^{-k}b_{k+1}) \frac{f(k)}{\psi(n, k+1, q)} \text{ for all } n \geq 0.$$

For the particular case $a_i = 1, b_i = 0$ for all i (and therefore $\psi(k, n, q) = 1$), this becomes

$$f(n) = \sum_{k=0}^n (-1)^k q^{\frac{k(k-1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q g(k) \quad (5)$$

if and only if

$$g(n) = \sum_{k=0}^n (-1)^k q^{\frac{k(k+1)}{2} - kn} \begin{bmatrix} n \\ k \end{bmatrix}_q f(k). \quad (6)$$

Putting $S(n) = f(n)$ and $T(n) = (-1)^n q^{\frac{n(n-1)}{2}} g(n)$, Eq. (5) becomes (3) and Eq. (6) becomes

$$\begin{aligned} \frac{T(n)}{(-1)^n q^{\frac{n(n-1)}{2}}} &= \sum_{k=0}^n (-1)^k q^{\frac{k(k+1)}{2} - kn} \begin{bmatrix} n \\ k \end{bmatrix}_q S(k) \\ T(n) &= \sum_{k=0}^n (-1)^{n+k} q^{\frac{n(n-1)}{2} + \frac{k(k+1)}{2} - kn} \begin{bmatrix} n \\ k \end{bmatrix}_q S(k) \\ &= \sum_{k=0}^n (-1)^{n-k} q^{\frac{(n-k)(n-k-1)}{2}} \begin{bmatrix} n \\ n-k \end{bmatrix}_q S(k). \end{aligned}$$

After replacing the index of summation k with $n-k$ in the last equation, we obtain precisely Eq. (4). \square

We will exploit invariance to linear (affine) invertible changes of coordinates:

Lemma 3 Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. The numbers $\dim(\text{FP}^{(\ell)}(f))$, $\ell = 1, 2, \dots, d$ are affine invariants, i.e. $\dim(\text{FP}^{(\ell)}(f)) = \dim(\text{FP}^{(\ell)}(f \circ \varphi))$ for any $\varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ which is an affine invertible change of coordinate.

Proof Using Lemma 1 we have that $a \in \text{FP}^{(\ell)}(f)$ iff $\varphi^{-1}(a) \in \text{FP}^{(\ell)}(f \circ \varphi)$. Therefore $\text{FP}^{(\ell)}(f \circ \varphi) = \varphi^{-1}(\text{FP}^{(\ell)}(f))$ hence $\dim(\text{FP}^{(\ell)}(f \circ \varphi)) = \dim(\text{FP}^{(\ell)}(f))$. \square

Corollary 1 Let $U \subseteq \mathbb{F}_2^n$ be a space of dimension k . The cardinality of $F^{(\ell)}(n, d; U)$ depends on the dimension of U but not on the space U itself. In particular

$$|F^{(\ell)}(n, d; U)| = |F^{(\ell)}(n, d; \langle e_{n-k+1}, \dots, e_n \rangle)|.$$

The functions f in n variables for which the space of fast points of order ℓ is generated by vectors in the canonical basis, $\langle e_{n-k+1}, \dots, e_n \rangle$ are, essentially, functions in fewer variables, i.e. they actually do not depend on x_{n-k+1}, \dots, x_n . More precisely, we can do the following reduction:

Lemma 4 Let $0 \leq k \leq n - d$. Then

$$|F^{(\ell)}(n, d; \langle e_{n-k+1}, \dots, e_n \rangle)| = |F^{(\ell)}(n - k, d; \{\mathbf{0}\})|$$

Proof For an equivalence class $[g]^{(d-\ell)}$ we can pick a representative which only contains monomials of degree $d, d - 1, \dots, d - \ell + 1$, where $d = \deg(g)$. Using Lemma 1(iv), we see that if $[g]^{(d-\ell)} \in F^{(\ell)}(n, d; \langle e_{n-k+1}, \dots, e_n \rangle)$ then the representative g which only contains monomials of degree $d, d - 1, \dots, d - \ell + 1$ does not depend on any of the variables x_{n-k+1}, \dots, x_n ; in other words, g is a polynomial in the $n - k$ variables x_1, \dots, x_{n-k} . Since the space of fast points of order ℓ of g is $\langle e_{n-k+1}, \dots, e_n \rangle$, this means that g has no non-trivial fast points when viewed as a function in the $n - k$ variables x_1, \dots, x_{n-k} , so we have $[g]^{(d-\ell)} \in F^{(\ell)}(n - k, d; \{\mathbf{0}\})$. Conversely, any function in $n - k$ variables in $F^{(\ell)}(n - k, d; \{\mathbf{0}\})$ can be viewed as a function in n variables and it has the required fast points to be in $F^{(\ell)}(n, d; \langle e_{n-k+1}, \dots, e_n \rangle)$. \square

We are now ready to count the functions which have a given space U (or any space of given dimension k) as their space of fast points of order 2.

Theorem 2 Let $0 \leq d \leq n$. For the cardinality of $F^{(2)}(., d, 0)$ (the set of functions of degree d with no fast points of order 2) we have the recurrence formula

$$\sum_{k=0}^{n-d} \binom{n}{k} |F^{(2)}(n - k, d; 0)| = (2^{\binom{n}{d}} - 1) 2^{\binom{n}{d-1}} \quad (7)$$

and the explicit formula

$$|F^{(2)}(n, d; 0)| = \sum_{i=0}^{n-d} (-1)^i 2^{\frac{i(i-1)}{2}} \binom{n}{i} \left(2^{\binom{n-i}{d}} - 1 \right) 2^{\binom{n-i}{d-1}}. \quad (8)$$

We also have, for any $0 \leq k \leq n - d$ and any space U of dimension k :

$$|F^{(2)}(n, d; U)| = \sum_{i=0}^{n-k-d} (-1)^i 2^{\frac{i(i-1)}{2}} \binom{n-k}{i} \left(2^{\binom{n-k-i}{d}} - 1 \right) 2^{\binom{n-k-i}{d-1}}, \quad (9)$$

$$|F^{(2)}(n, d; k)| = \binom{n}{k} \sum_{i=0}^{n-k-d} (-1)^i 2^{\frac{i(i-1)}{2}} \binom{n-k}{i} \left(2^{\binom{n-k-i}{d}} - 1 \right) 2^{\binom{n-k-i}{d-1}}. \quad (10)$$

Proof For the recurrence relation, consider the set of functions of degree d in n variables. This set can be partitioned into subsets according to their space of fast points of order 2, i.e. each function f belongs to the set $F^{(2)}(n, d; U)$ where U is the space of fast points of order 2 of f . This means

$$\bigcup_U F^{(2)}(n, d; U) = \{[f]^{(d-2)} : f \in B(n, d)\}$$

where the union is over U ranging over all subspaces of \mathbb{F}_2^n of dimension at most $n - d$ (recall that spaces of fast points can have dimension at most $n - d$). The cardinality of the set on the right hand side is $(2^{\binom{n}{d}} - 1)2^{\binom{n}{d-1}}$, since for any class we can pick the representative which only has monomials of degree d and $d - 1$; there are $\binom{n}{d}$ monomials of degree d , and each of them can have a coefficient of 0 or 1; however, the situation of all-zero coefficients is excluded as the degree of f must be d . There are $\binom{n}{d-1}$ monomials of degree $d - 1$, each with coefficient 0 or 1 (this time with the possibility of all coefficients being 0). For computing the cardinality of the set on the left hand side, using the fact that the sets are disjoint we have:

$$|\bigcup_U F^{(2)}(n, d; U)| = \sum_U |F^{(2)}(n, d; U)| = \sum_{k=0}^{n-d} \sum_{\dim(U)=k} |F^{(2)}(n, d; U)|.$$

Using Corollary 1 and Lemma 4 and the fact that there are $\begin{bmatrix} n \\ k \end{bmatrix}$ subspaces of each dimension k , we have

$$|\bigcup_U F^{(2)}(n, d; U)| = \sum_{k=0}^{n-d} \begin{bmatrix} n \\ k \end{bmatrix} |F^{(2)}(n - k, d; 0)|$$

which completes the proof of the recurrence relation (7).

For the proof of the first explicit formula we rewrite (7) as

$$\begin{aligned} \sum_{k=0}^{n-d} \begin{bmatrix} n \\ k \end{bmatrix} |F^{(2)}(n - k, d; 0)| &= \sum_{k=0}^n \begin{bmatrix} n \\ n - k \end{bmatrix} |F^{(2)}(n - k, d; 0)| \\ &= \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} |F^{(2)}(k, d; 0)| \\ &= (2^{\binom{n}{d}} - 1)2^{\binom{n}{d-1}} \end{aligned}$$

using the fact that $|F^{(2)}(k, d; 0)| = 0$ when $k < d$. This recurrence relation is of the type of equation (3) in Lemma 2, viewing d as fixed and putting $S(n) = (2^{\binom{n}{d}} - 1)2^{\binom{n}{d-1}}$ and $T(n) = |F^{(2)}(n, d; 0)|$. Therefore, equation (4) in Lemma 2 gives the first explicit formula (8) in the theorem statement (with the summation going up to n , but then note that $S(n - i) = 0$ for $n - d < i \leq n$).

Alternatively, (8) could also be proven using the technique from the proof of [13, Theorem 6].

For the next explicit formula (9), we use Eq. (8), Corollary 1 and Lemma 4. Finally for the final formula (10) we use the fact that $F^{(2)}(n, d; k) = \bigcup_U F^{(2)}(n, d; U)$ where U ranges over all the $\begin{bmatrix} n \\ k \end{bmatrix}$ spaces of dimension k in \mathbb{F}_2^n and the sets in the union are disjoint. \square

The Theorem above can be generalised to counting the functions which have a given space U (or any space of given dimension k) as their space of fast points of order ℓ .

Theorem 3 *Let $1 \leq \ell \leq d$, $0 \leq k \leq n - d$ and let U be a space of dimension k . Then*

$$|F^{(\ell)}(n, d; U)| = \sum_{i=0}^{n-k-d} (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n - k \\ i \end{bmatrix} (2^{\binom{n-k-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} \binom{n-k-i}{d-j}} \quad (11)$$

and

$$|F^{(\ell)}(n, d; k)| = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{i=0}^{n-k-d} (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n - k \\ i \end{bmatrix} (2^{\binom{n-k-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} \binom{n-k-i}{d-j}}. \quad (12)$$

Furthermore, the number of functions which have fast points of order ℓ (any number of non-trivial fast points of order ℓ) is:

$$\begin{aligned} & |\{[f]^{(d-\ell)} : f \in B(n, d), \text{FP}^{(\ell)}(f) \neq \{\mathbf{0}\}\}| \\ &= \sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \left(2^{\binom{n-i}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n-i}{d-j}}. \end{aligned} \quad (13)$$

Proof As in the proof of Theorem 2, we have

$$\bigcup_U \text{F}^{(\ell)}(n, d; U) = \{[f]^{(d-\ell)} | f \in B(n, d)\}.$$

as the set of functions of degree d in n variables can be partitioned into the sets $\text{F}^{(\ell)}(n, d; U)$ with U ranging over all subspaces of \mathbb{F}_2^n of dimension up to $n - d$. For the cardinality of the right hand side we have:

$$|\{[f]^{(d-\ell)} : f \in B(n, d)\}| = \left(2^{\binom{n}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n}{d-j}}.$$

Using Corollary 1 and Lemma 4 for the cardinality of the left hand side we obtain:

$$\begin{aligned} |\bigcup_U \text{F}^{(\ell)}(n, d; U)| &= \sum_U |\text{F}^{(\ell)}(n, d; U)| \\ &= \sum_{k=0}^{n-d} \sum_{\dim(U)=k} |\text{F}^{(\ell)}(n, d; U)| \\ &= \sum_{k=0}^{n-d} \begin{bmatrix} n \\ k \end{bmatrix} |\text{F}^{(\ell)}(n - k, d; 0)|. \end{aligned}$$

Putting these together we obtain the recurrence relation

$$\sum_{k=0}^{n-d} \begin{bmatrix} n \\ k \end{bmatrix} |\text{F}^{(\ell)}(n - k, d; 0)| = \left(2^{\binom{n}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n}{d-j}}$$

which we solve using Lemma 2 to obtain

$$|\text{F}^{(\ell)}(n, d; 0)| = \sum_{i=0}^{n-d} (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \left(2^{\binom{n-i}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n-i}{d-j}}.$$

Using this formula and Lemma 4, we then obtain (11) and (12).

For Eq. (13) we have:

$$\begin{aligned} & |\{[f]^{(d-\ell)} : f \in B(n, d), \text{FP}^{(\ell)}(f) \neq \{\mathbf{0}\}\}| \\ &= |\{[f]^{(d-\ell)} : f \in B(n, d)\} \setminus \text{F}^{(\ell)}(n, d; 0)| \\ &= \left(2^{\binom{n}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n}{d-j}} - \sum_{i=0}^{n-d} (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \left(2^{\binom{n-i}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n-i}{d-j}} \\ &= \sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \left(2^{\binom{n-i}{d}} - 1\right) 2^{\sum_{j=1}^{\ell-1} \binom{n-i}{d-j}}. \end{aligned}$$

□

4 Applications

As a first application of these counting results, we can determine the number of functions which have linear structures. An element $a \in \mathbb{F}_2^n \setminus \{0\}$ is a *linear structure* for a function f if $D_a f$ is a constant function. With our definition, a linear structure for f is a fast point of order $\deg(f) - 1$. Therefore, applying Theorem 3 we have:

Corollary 2 *The number of functions of degree d in n variables which have linear structures is:*

$$\sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \left(2^{\binom{n-i}{d}} - 1 \right) 2^{\sum_{j=1}^{d-2} \binom{n-i}{d-j}}.$$

where the functions are counted up to addition of an affine function.

Example 1 Let $n = 7, d = 3$. We compute the number of functions of degree 3 in 7 variables which have fast points of order 2, i.e. they have linear structures. Using Corollary 2, this number is:

$$\sum_{i=1}^4 (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} 7 \\ i \end{bmatrix} \left(2^{\binom{7-i}{3}} - 1 \right) 2^{\binom{7-i}{2}} = 4,358,179,630,080.$$

Note the counting is done up to equivalence $\stackrel{(1)}{\sim}$ i.e. up to addition of affine functions. The remaining

$$\begin{aligned} \left(2^{\binom{7}{3}} - 1 \right) 2^{\binom{7}{2}} - 4,358,179,630,080 &= 72,057,594,035,830,784 - 4,358,179,630,080 \\ &= 72,053,235,856,200,704 \end{aligned}$$

functions have no linear structures. We can also compute the number of functions with no fast points of order 2 directly using Theorem 2:

$$|F^{(2)}(7, 3; 0)| = \sum_{i=0}^4 (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} 7 \\ i \end{bmatrix} \left(2^{\binom{7-i}{3}} - 1 \right) 2^{\binom{7-i}{2}} = 72,053,235,856,200,704.$$

The proportion of functions which have linear structures out of all functions of degree 3 in 7 variables is

$$\frac{4,358,179,630,080}{72,057,594,035,830,784} \approx 0.000061035.$$

In other words, if we pick a function of degree 3 in 7 variables uniformly at random, the probability that it has a linear structure is approximately 0.00006.

As a second application of our counting results we estimate various probabilities for functions to have faster points (in particular, to have linear structures), similar to the estimates in [13].

Proposition 1 *Assume a function f is chosen uniformly at random among the functions of degree d in n variables. Let $1 \leq \ell \leq d$.*

The probability that f has at least one fast point of order ℓ is

$$\begin{aligned} & \frac{|\{[f]^{(d-\ell)} : f \in B(n, d), \text{FP}^{(\ell)}(f) \neq \{\mathbf{0}\}\}|}{|\{[f]^{(d-\ell)} : f \in B(n, d)\}|} \\ &= \sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} \frac{2^{\binom{n-i}{d}} - 1}{2^{\binom{n}{d}} - 1} 2^{\sum_{j=1}^{\ell-1} (\binom{n-i}{d-j} - \binom{n}{d-j})}. \end{aligned}$$

When $d - \ell \geq 2$ and $n - d \geq 3$, this can be approximated as

$$\frac{1}{2^{-n+\sum_{j=1}^{\ell} \binom{n-1}{d-j}}} \quad (14)$$

The conditional probability that f has at least one fast point of order ℓ knowing that it does have fast points of order $\ell - 1$ (for $\ell > 1$) is

$$\begin{aligned} & \frac{|\{[f]^{(d-\ell)} : f \in B(n, d), \text{FP}^{(\ell)}(f) \neq \{\mathbf{0}\}\}|}{|\{[f]^{(d-\ell)} : f \in B(n, d), \text{FP}^{(\ell-1)}(f) \neq \{\mathbf{0}\}\}|} \\ &= \frac{\sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} (2^{\binom{n-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} (\binom{n-i}{d-j} - \binom{n}{d-j})}}{2^{\binom{n}{d-\ell+1}} \sum_{i=1}^{n-d} (-1)^{i-1} 2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} (2^{\binom{n-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-2} (\binom{n-i}{d-j} - \binom{n}{d-j})}} \end{aligned}$$

When $d - \ell \geq 2$ and $n - d \geq 3$, this can be approximated as

$$\frac{1}{2^{\binom{n-1}{d-\ell}}}$$

Proof For the first equation, we use Theorem 3 and the fact that

$$|\{[f]^{(d-\ell)} : f \in B(n, d)\}| = (2^{\binom{n}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} \binom{n}{d-j}}.$$

For the second equation, note that in the denominator we have equivalence classes $[f]^{(d-\ell)}$ for fast points of order $\ell - 1$, so we need to multiply by $2^{\binom{n}{d-\ell+1}}$ the result obtained by replacing ℓ by $\ell - 1$ in (13).

For the approximations, we note that in the sum (13), the terms have alternating signs and decrease rapidly in absolute value, so the sum can be approximated by its first term. Namely, the ratio of the absolute values of term $i + 1$ to the term i is:

$$\begin{aligned} & \frac{2^{\frac{i(i+1)}{2}} \begin{bmatrix} n \\ i+1 \end{bmatrix} (2^{\binom{n-i-1}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} (\binom{n-i-1}{d-j} - \binom{n}{d-j})}}{2^{\frac{i(i-1)}{2}} \begin{bmatrix} n \\ i \end{bmatrix} (2^{\binom{n-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} (\binom{n-i}{d-j} - \binom{n}{d-j})}} = \frac{2^i (2^{n-i} - 1) (2^{\binom{n-i-1}{d}} - 1)}{(2^{i+1} - 1) (2^{\binom{n-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} (\binom{n-i}{d-j} - \binom{n-i-1}{d-j})}} \\ &= \frac{2^i (2^{n-i} - 1) (2^{\binom{n-i-1}{d}} - 1)}{(2^{i+1} - 1) (2^{\binom{n-i}{d}} - 1) 2^{\sum_{j=1}^{\ell-1} (\binom{n-i}{d-j-1} - \binom{n-i-1}{d-j-1})}} \\ &\approx \frac{1}{2^{-n+i+1+\sum_{j=0}^{\ell-1} \binom{n-i-1}{d-j-1}}} \end{aligned}$$

which is negligible provided $d - \ell \geq 2$ and $n - d \geq 3$. \square

Example 2 For the computation in Example 1 above, if we use instead Proposition 1 (14) to estimate the probability of a function of degree 3 in 7 variables to have a linear structure we obtain:

$$\frac{1}{2^{-7+\binom{6}{2}+\binom{6}{1}}} = \frac{1}{2^{14}}$$

which has an error of less than 1% compared to the precise value computed in Example 1.

5 Counting the number of functions with a given profile of fast points of different orders

Next we will refine the counting so that we can count functions where the spaces of fast points of each order are specified. For \mathbb{F}_2 -linear subspaces of the form $\mathbb{F}_2^n \supseteq U_1 \supseteq U_2 \cdots \supseteq U_\ell \supseteq \{0\}$ with $1 \leq \ell \leq d$ we denote

$$F^{(\ell)}(n, d; U_1, U_2, \dots, U_\ell) = \{[f]^{(d-\ell)} : f \in \text{BF}(n, d), \text{FP}^{(i)}(f) = U_i \text{ for } 1 \leq i \leq \ell\}.$$

More generally, keeping in mind that the dimensions of the spaces of fast points of each order for a function f are affine invariants (see Lemma 3), we define for integers $n - d \geq k_1 \geq k_2 \geq \dots \geq k_\ell \geq 0$:

$$F^{(\ell)}(n, d; k_1, k_2, \dots, k_\ell) = \{[f]^{(d-\ell)} : f \in \text{BF}(n, d), \dim(\text{FP}^{(i)}(f)) = k_i \text{ for } 1 \leq i \leq \ell\}.$$

We will determine the cardinalities of the sets above. Similarly to Corollary 1 we have

$$|F^{(\ell)}(n, d; U_1, U_2, \dots, U_\ell)| = |F^{(\ell)}(n, d; W_{k_1}, W_{k_2}, \dots, W_{k_\ell})| \quad (15)$$

where $k_i = \dim(U_i)$ and $W_{k_i} = \langle e_{n-k_i+1}, \dots, e_n \rangle$, with e_i being the canonical basis vectors and $W_0 = \{0\}$ by convention.

Let us examine an element $f \in F^{(\ell)}(n, d; W_{k_1}, W_{k_2}, \dots, W_{k_\ell})$. We can assume that the representative f only contains monomials of degree $d, d-1, \dots, d-\ell+1$. Write $f = f_d + f_{d-1} + \dots + f_{d-\ell+1}$, with each f_i containing only monomials of degree i (i.e. f_i is the homogeneous part of degree i of f). Using Lemma 1(iv) we see that f_d does not contain any of the variables x_{n-k_1+1}, \dots, x_n ; f_{d-1} does not contain any of the variables x_{n-k_2+1}, \dots, x_n etc. Moreover f_d does not have any fast points (of any order) when viewed as a function in $n-k_1$ variables. For f_{d-1} the situation is less straightforward; when viewed as a function in $n-k_2$ variables, it can have fast points, but any such points have to be outside $\langle e_{n-k_1+1}, \dots, e_{n-k_2} \rangle$.

We will therefore need to count functions which *do not* have fast points within a certain specified space. We define $X_k(n, d)$ with $0 \leq k \leq d \leq n$ as the set of functions f of degree d in n variables such that none of the non-zero elements of the space W_k is a fast point for f (note that f may have non-trivial fast points, but only if they are outside W_k). We also include $f = 0$ in the set $X_k(n, d)$. More precisely:

$$X_k(n, d) = \{[f]^{(d-1)} : f \in \text{BF}(n, d) \text{ and } \text{FP}^{(1)}(f) \cap W_k = \{0\}\} \cup \{[0]^{(d-1)}\}.$$

The cardinality of the set $X_k(n, d)$ would remain the same if in the definition of $X_k(n, d)$ we replace the space W_k by any space U of dimension k :

$$|X_k(n, d)| = |\{[f]^{(d-1)} : f \in \text{BF}(n, d) \text{ and } \text{FP}^{(1)}(f) \cap U = \{0\}\} \cup \{[0]^{(d-1)}\}|. \quad (16)$$

One can generalise this further by fixing two spaces $U_1 \subseteq U_0$ and considering the functions f with the property that the points in U_1 are fast points of f but no other points of U_0 are fast

points of f . Note that we do not care how many fast points f has outside U_0 . The cardinality of this set can be expressed using the sets $X_k(n, d)$ as follows:

Lemma 5 *Let $U_1 \subseteq U_0$ be two subspaces of \mathbb{F}_2^n of dimension k_1 and k_0 respectively.*

$$|\{[f]^{(d-1)} : f \in \text{BF}(n, d) \text{ and } \text{FP}^{(1)}(f) \cap U_0 = U_1\} \cup \{[0]^{(d-1)}\}| = |X_{k_0-k_1}(n-k_1, d)|$$

Proof Let us first consider the particular case $U_0 = W_{k_0}$ and $U_1 = W_{k_0}$. Let f be a function such that $\text{FP}^{(1)}(f) \cap U_0 = U_1$. Since we are only interested in the equivalence class $[f]^{(d-1)}$, we can assume f only contains monomials of degree d . Since the elements of U_1 are fast points for f , by Lemma 1(iv) this means f does not contain any of the variables x_{n-k_1+1}, \dots, x_n ; it is a polynomial in the remaining $n-k_1$ variables x_1, \dots, x_{n-k_1} . We now determine $\text{FP}^{(1)}(f) \cap V$ where $V = \langle e_{n-k_0+1}, \dots, e_{n-k_1} \rangle$. Since we have $\text{FP}^{(1)}(f) \cap V \subseteq \text{FP}^{(1)}(f) \cap U_0 = U_1$, we deduce $\text{FP}^{(1)}(f) \cap V \subseteq U_1 \cap V = \{0\}$. Hence $[f]^{(d-1)} \in X_{k_0-k_1}(n-k_1, d)$.

Conversely, let f be such that $[f]^{(d-1)} \in X_{k_0-k_1}(n-k_1, d)$. We can view f as a function in n variables, i.e. we can define a function g as $g(x_1, \dots, x_n) = f(x_1, \dots, x_{n-k_1})$. Since g does not depend on x_{n-k_1+1}, \dots, x_n , we have that $U_1 \subseteq \text{FP}^{(1)}(g)$. On the other hand, $\text{FP}^{(1)}(g) \cap V = \{0\}$ because $[f]^{(d-1)} \in X_{k_0-k_1}(n-k_1, d)$. Therefore $\text{FP}^{(1)}(g) \cap U_0 = U_1$.

For the general case, consider a basis a_{n-k_0+1}, \dots, a_n for U_0 such that a_{n-k_1+1}, \dots, a_n is a basis for U_1 . Consider an affine transformation $\varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ such that $\varphi(e_i) = a_i$ for $i = n-k_0+1, \dots, n$. Let f be such that $\text{FP}^{(1)}(f) \cap U_0 = U_1$. By Lemma 1, this happens iff $f \circ \varphi$ is such that $\text{FP}^{(1)}(f \circ \varphi) \cap \varphi^{-1}(U_0) = \varphi^{-1}(U_1)$, i.e. $\text{FP}^{(1)}(f \circ \varphi) \cap W_{k_0} = W_{k_1}$. We then use the first part of the proof. \square

Proposition 2 *The following formula holds:*

$$\sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix} |X_{k-i}(n-i, d)| = 2^{\binom{n}{d}}.$$

Therefore for each fixed d we can obtain $|X_k(n, d)|$ by the following recursive formulae (recursion on both k and n):

$$|X_k(n, d)| = 2^{\binom{n}{d}} - \sum_{i=1}^k \begin{bmatrix} k \\ i \end{bmatrix} |X_{k-i}(n-i, d)|$$

with initial conditions $|X_0(n, d)| = 2^{\binom{n}{d}}$.

Proof For $k = 0$, we obviously have $X_0(n, d) = \{[f]^{(d-1)} : f \in \text{BF}(n, d)\} \cup \{0\}$ so $|X_0(n, d)| = 2^{\binom{n}{d}}$. For arbitrary k we have:

$$\begin{aligned} & \{[f]^{(d-1)} : f \in \text{BF}(n, d) \cup \{0\}\} \\ &= \bigcup_{V \subseteq W_k} \{[f]^{(d-1)} : f \in \text{BF}(n, d) \text{ and } \text{FP}^{(1)}(f) \cap W_k = V\} \cup \{[0]^{(d-1)}\} \end{aligned}$$

where V ranges over all subspaces of W_k ; for each dimension i there are $\begin{bmatrix} k \\ i \end{bmatrix}$ such spaces. Note that the sets in the union are pairwise disjoint and by Lemma 5 they have $|X_{k-\dim(V)}(n-\dim(V), d)|$ elements each, so

$$2^{\binom{n}{d}} = \sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix} |X_{k-i}(n-i, d)|.$$

\square

Proposition 3 *The following explicit formulae for $|X_k(n, d)|$ hold:*

$$|X_k(n, d)| = \sum_{i=0}^k (-1)^i 2^{\frac{i(i-1)}{2}} \begin{bmatrix} k \\ i \end{bmatrix} 2^{\binom{n-i}{d}} \quad (17)$$

and

$$|X_k(n, d)| = \sum_{i=0}^{n-k} 2^{ik} \begin{bmatrix} n-k \\ i \end{bmatrix} |\mathbb{F}^{(1)}(n-i, d, 0)| \quad (18)$$

Proof For the first formula, the recurrence relation from Proposition 2 becomes, after replacing the index of summation by $j = k - i$

$$\sum_{j=0}^k \begin{bmatrix} k \\ j \end{bmatrix} |X_j(n-k+j, d)| = 2^{\binom{n-k+k}{d}}.$$

It then satisfies the conditions from Eq. (3) in Lemma 2, considering d and $n - k$ fixed and putting $T(j) = |X_j(n - k + j, d)|$ and $S(j) = 2^{\binom{n-k+j}{d}}$. Equation (4) in Lemma 2 gives then the first explicit formula.

Alternatively, we could have used the same technique as in the proof of [13, Theorem 6].

For the second formula in the theorem statement we use a different approach, counting the cardinality of $X_k(n, d)$ directly. First let us count the number of subspaces V of \mathbb{F}_2^n of dimension i such that $V \cap W_k = \{\mathbf{0}\}$. This latter condition implies $0 \leq i \leq n - k$. To pick a basis v_1, \dots, v_i for such a space V we have $2^n - 2^k$ possibilities to pick $v_1 \in \mathbb{F}_2^n \setminus W_k$, then $2^n - 2^{k+1}$ possibilities to pick $v_2 \in \mathbb{F}_2^n \setminus \langle W_k, v_1 \rangle$ etc. However, this way each space V ends up being counted $(2^i - 1)(2^i - 2) \dots (2^n - 2^{i-1})$ times (the number of bases of V , taking into account the ordering of the basis elements). So altogether the number of spaces is

$$\frac{(2^n - 2^k)(2^n - 2^{k+1}) \dots (2^n - 2^{k+i-1})}{(2^i - 1)(2^i - 2) \dots (2^i - 2^{i-1})} = 2^{ik} \begin{bmatrix} n-k \\ i \end{bmatrix}$$

For each such space V , there are $|\mathbb{F}^{(1)}(n, d; V)| = |\mathbb{F}^{(1)}(n - i, d; 0)|$ functions which have V as their set of fast points. Putting everything together we obtain formula (18). \square

We can now move to determining the number of functions with prescribed spaces (or prescribed dimensions of spaces) of fast points of each order.

Theorem 4 *Let $1 \leq \ell \leq d \leq n$ and $n - d \geq k_1 \geq k_2 \geq \dots \geq k_\ell \geq 0$, and let vector spaces $U_1 \supseteq U_2 \supseteq \dots \supseteq U_\ell$, with $k_i = \dim(U_i)$. Put $k_0 = n$. We have*

$$|\mathbb{F}^{(\ell)}(n, d; U_1, \dots, U_\ell)| = |\mathbb{F}^{(1)}(n - k_1, d; 0)| \prod_{i=1}^{\ell-1} |X_{k_i - k_{i+1}}(n - k_{i+1}, d - i)|$$

and

$$|\mathbb{F}^{(\ell)}(n, d; k_1, k_2, \dots, k_\ell)| = |\mathbb{F}^{(1)}(n - k_1, d; 0)| \left(\prod_{i=1}^{\ell} \begin{bmatrix} k_{i-1} \\ k_i \end{bmatrix} \right) \left(\prod_{i=1}^{\ell-1} |X_{k_i - k_{i+1}}(n - k_{i+1}, d - i)| \right)$$

where $|\mathbb{F}^{(1)}(\cdot)|$ is computed using Theorem 1 and $|X(\cdot)|$ are computed using Proposition 3.

Proof We continue the proof started at the beginning of this section. By Eq. (15) it suffices to deal with the case when $U_i = W_{k_i}$ for $i = 1, \dots, \ell$. For any class $[f]^{(d-\ell)}$ we can assume that all the monomials of f have degrees between d and $d - \ell + 1$ inclusive. Write f as $f = f_d + f_{d-1} + \dots + f_{d-\ell+1}$ where each f_i is a homogeneous polynomial of degree i ; for $i < d$, f_i can also be zero.

We will show that $[f]^{(d-\ell)} \in F^{(\ell)}(n, d; W_{k_1}, \dots, W_{k_\ell})$ iff $f_d \in F^{(1)}(n, d; W_{k_1})$ and $f_{d-i+1} \in \{[g]^{(d-i)} : f \in \text{BF}(n, d) \text{ and } \text{FP}^{(1)}(g) \cap W_{k_{i-1}} = W_{k_i}\} \cup \{[0]^{(d-i)}\}$ for $i = 2, \dots, \ell$. The counting formula will then follow using Lemma 5.

For the direct implication, let $[f]^{(d-\ell)} \in F^{(\ell)}(n, d; W_{k_1}, \dots, W_{k_\ell})$, i.e. $\text{FP}^{(i)} f = W_{k_i}$ for $i = 1, \dots, \ell$. By Lemma 1(iv), we have that f_{d-i+1} does not contain the variables x_{n-k_i+1}, \dots, x_n . If f_d had any fast points of order 1 outside W_{k_1} , then those would also be fast points of order 1 for f , so indeed we must have $\text{FP}^{(1)}(f_d) = W_{k_1}$. Now let us examine f_{d-i+1} for $i > 1$. If $f_{d-i+1} = 0$ we are done. Otherwise, since f_{d-i+1} does not contain the variables x_{n-k_i+1}, \dots, x_n , we have that $W_{k_i} \subseteq \text{FP}^{(1)}(f_{d-i+1})$. Assume $a \in \text{FP}^{(1)}(f_{d-i+1}) \cap W_{k_{i-1}}$. We have

$$\begin{aligned} D_a f &= D_a f_d + \dots + D_a f_{d-i+2} + D_a f_{d-i+1} + D_a f_{d-i} + \dots + D_a f_{d-\ell+1} \\ &= D_a f_{d-i+1} + D_a f_{d-i} + \dots + D_a f_{d-\ell+1} \end{aligned} \quad (19)$$

since $a \in W_{k_{i-1}}$ and the first i functions do not contain the variables $x_{n-k_{i-1}+1}, \dots, x_n$. Therefore, $\deg(D_a f_{d-i+1}) < \deg(f_{d-i+1}) - 1 = d - i$ iff $\deg(D_a f) < d - i$ iff $a \in \text{FP}^{(i)}(f) = W_{k_i}$.

For the reverse implication, assume f is such that $\text{FP}^{(1)}(f_d) = W_{k_1}$ and f_{d-i+1} are such that either $f_{d-i+1} = 0$ or $\text{FP}^{(1)}(f_{d-i+1}) \cap W_{k_{i-1}} = W_{k_i}$. We have to show $\text{FP}^{(i)}(f) = W_{k_i}$ for $i = 1, \dots, \ell$. Since $W_{k_i} \subseteq \text{FP}^{(1)}(f_{d-i+1})$ for $i = 1, \dots, \ell$, we know that f_{d-i+1} does not contain the variables x_{n-k_i+1}, \dots, x_n , so we have $W_{k_i} \subseteq \text{FP}^{(i)}(f)$. Now let $a \in \text{FP}^{(i)}(f)$. By induction on i we show that $a \in W_{k_i}$. For $i = 1$ we have that a is a fast point of order 1 for f , which means it is also a fast point of order 1 for f_d , so $a \in \text{FP}^{(1)}(f_d) = W_{k_1}$. For the inductive step, note that if a is a fast point of order i for f , then it is also a fast point of order $i - 1$, so by the induction hypothesis $a \in W_{k_{i-1}}$. Therefore, as in (19), a is a fast point of order i for f iff $f_{d-i+1} = 0$ or a is a fast point of order 1 for f_{d-i+1} , hence $a \in W_{k_{i-1}} \cap \text{FP}^{(1)}(f_{d-i+1}) = W_{k_i}$. \square

We therefore have now an alternative to Theorem 2 for computing $F^{(2)}(n, d; 0)$:

Corollary 3

$$|F^{(2)}(n, d; 0)| = \sum_{k=0}^{n-d} \begin{bmatrix} n \\ k \end{bmatrix} X_k(n, d-1) |F^{(1)}(n-k, d, 0)|$$

Proof Use Theorem 4 combined with

$$F^{(2)}(n, d; 0) = \bigcup_U F^{(2)}(n-k, d; U, 0)$$

where U ranges over all subspaces of \mathbb{F}_2^n ; the sets in the union are disjoint. \square

Example 3 Let $n = 7, d = 3$. We compute the number of functions (up to equivalence) of degree 3 in 7 variables which have no fast points of order 2 using Corollary 3:

$$|F^{(2)}(7, 3; 0)| = \sum_{k=0}^4 \begin{bmatrix} 7 \\ k \end{bmatrix} X_k(7, 2) |F^{(1)}(7 - k, 3, 0)|$$

Using the values of $|F^{(1)}(7 - k, 3, 0)|$ computed in [13], we obtain 72,053,235,856,200,704, same as in Example 1.

6 Conclusion

Motivated by the properties of cryptographic functions exploited by differential attacks, Duan and Lai [6] introduced the notion of Boolean functions that admit “fast points”. We generalised this notion, defining functions f which have “fast points of order ℓ ” i.e. the degree of at least one of the discrete derivatives of f is lower by ℓ than the expected value (i.e. it is $d - 1 - \ell$ or less, instead of the expected $d - 1$, where d is the algebraic degree of f). We obtained explicit formulae for the number of such functions of degree d in n variables. As an important particular case, this allowed us to compute the number of functions which admit a linear structure. Moreover, we computed the number of functions which have a given profile in terms of the number of fast points of each order.

Acknowledgements The authors thank to Royal Society for their support through the Newton Mobility Grant NI170158. During their visits, the authors benefited from the hospitality of the Department of Computer Science, Loughborough University as well as the Department of Mathematics, Middle East Technical University, Ankara. The authors also thank Julien Lavauzelle for pointing them in the right direction regarding the origin of Lemma 2. We also thank the reviewers for careful comments which led to improvements to the paper.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Abdul-Latip S.F., Reyhanitabar M.R., Susilo W., Seberry J.: Extended cubes: enhancing the cube attack by extracting low-degree non-linear equations. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, pp. 296–305 (2011).
2. Aumasson J.-P., Dinur I., Meier W., Shamir A.: Cube testers and key recovery attacks on reduced-round MD6 and Trivium. In: Fast Software Encryption—16th International Workshop, FSE, pp. 1–22 (2009).
3. Carlitz L.: Some inverse relations. Duke Math. J. **40**(4), 893–901 (1973).
4. Chaum D., Evertse J.-H.: Cryptanalysis of DES with a reduced number of rounds. In: Proceedings of Crypto '85, pp. 192–211 (1985).
5. Dinur I., Shamir A.: Cube attacks on tweakable black box polynomials. In: EUROCRYPT, pp. 278–299 (2009).
6. Duan M., Lai X.: Higher order differential cryptanalysis framework and its applications. In: International Conference on Information Science and Technology (ICIST), pp. 291–297 (2011).
7. Duan M., Yang M., Sun X., Zhu B., Lai Xuejia: Distinguishing properties and applications of higher order derivatives of Boolean functions. Inf. Sci. **271**, 224–235 (2014).
8. Fouque, P.-A., Vannet, T.: Improving key recovery to 784 and 799 rounds of Trivium using optimized cube attacks. In: Fast Software Encryption—20th International Workshop, FSE 2013, Singapore, March 11–13, 2013. Revised Selected Papers, pp. 502–517 (2013).
9. Hou X.: $GL(m, 2)$ acting on $R(r, m)/R(r - 1, m)$. Discret. Math. **149**(1), 99–122 (1996).

10. Lai X.: Higher order derivatives and differential cryptanalysis. In: Blahut R.E., Costello Jr. D.J., Maurer U., Mittelholzer T. (eds.) *Communications and Cryptography*, vol. 276, pp. 227–233. The Springer International Series in Engineering and Computer Science Springer, New York (1994).
11. Langevin P., Leander G.: Classification of the quartic forms of eight variables. In: *Boolean Functions in Cryptology and Information Security*, Svenigorod (2007).
12. Online Encyclopedia of Integer Sequences. <https://oeis.org>.
13. Sălăgean A., Mandache-Sălăgean M.: Counting and characterising functions with “fast points” for differential attacks. *Cryptogr. Commun.* **9**, 217–239 (2015).
14. Vielhaber M.: Breaking ONE.FIVIUM by AIDA an algebraic IV differential attack. *Cryptology ePrint Archive*, Report 2007/413. <http://eprint.iacr.org/> (2007).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.