A Degree Bound for the c-Boomerang Uniformity

Matthias Johann Steiner
Alpen-Adria-Universität Klagenfurt,
Universitätsstraße 65-67, 9020 Klagenfurt am Wörthersee, Austria
mattsteiner@edu.aau.at

Abstract

Let $\mathbb{F}_q$ be a finite field, and let $F \in \mathbb{F}_q[X]$ be a polynomial with $d = \deg(F)$ such that $\gcd(d, q) = 1$. In this paper we prove that the c-Boomerang uniformity, $c \neq 0$, of F is bounded by $\begin{cases} d^2, & c^2 \neq 1, \\ d \cdot (d-1), & c = -1, \\ d \cdot (d-2), & c = 1 \end{cases}$. For all cases of c, we present tight examples for $F \in \mathbb{F}_q[X]$.

Additionally, for the proof of $c = 1$ we establish that the bivariate polynomial $F(x) - F(y) + a \in k[x, y]$, where k is a field of characteristic p and $a \in k \setminus \{0\}$, is absolutely irreducible if $p \nmid \deg(F)$.

1 Introduction

Differential cryptanalysis introduced by Biham & Shamir [1] studies the propagation of input differences through a symmetric key cipher or a hash function. The susceptibility of a function $F : \mathbb{F}_q \to \mathbb{F}_q$ against differential cryptanalysis is expressed in the *Differential Distribution Table* (DDT)

$$\delta_F(a, b) = \left|\left\{\mathbf{x} \in \mathbb{F}_q^n \mid F(x + a) - F(x) = b\right\}\right|, \tag{1}$$

where $a, b \in \mathbb{F}_q$. The maximum entry with $a \neq 0$ of the DDT is also known as *differential uniformity* [2]. In a recent work Ellingsen et al. [3] generalized the DDT to c-scaled differences.

A variant of differential cryptanalysis is the Boomerang attack introduced by Wagner [4]. In the spirit of the DDT, Cid et al. [5] introduced the *Boomerang Connectivity Table* (BCT) to quantify the resistance of a permutation $F : \mathbb{F}_q \to \mathbb{F}_q$ against the Boomerang attack. Analogous to the c-scaled DDT, Stănică [6] introduced c-scaled differences to the BCT

$${}_c\mathcal{B}_F(a, b) = \left|\left\{(x, y) \in \mathbb{F}_q^2 \;\middle|\; \begin{matrix} F(x + y) - c \cdot F(x) = b \\ c \cdot F(x + y + a) - F(x + a) = c \cdot b \end{matrix}\right\}\right|, \tag{2}$$

where $a, b \in \mathbb{F}_q$ and $c \in \mathbb{F}_q^\times$. The maximum entry of the c-BCT for $a, b \neq 0$ is also known as *c-Boomerang uniformity*.

Since its introduction, the c-BCT has been studied for many special permutation polynomials [6, 7, 8, 9, 10, 11]. However, the mathematical investigations into functions with low (c-)Boomerang uniformity are in stark contrast with the actual requirements of many modern symmetric cryptography primitives. The past decade has seen a fast development of cryptographic primitives and protocols with privacy enhancing features, such as Fully-Homomorphic Encryption (FHE),

Multi-Party Computation (MPC) and Zero-Knowledge (ZK) proofs. Performance of MPC, FHE & ZK can often be improved via a dedicated symmetric cipher or hash function. We provide an (incomplete) overview of proposed symmetric primitives for these applications:

- Ciphers and Pseudo-Random Functions for MPC [12]: `MiMC` [13], `GMiMC` [14], HADES [15], `Ciminion` [16], Hydra [17].
- Hash functions for ZK: `GMiMCHash` [14], POSEIDON [18], `Anemoi` [19], GRIFFIN [20], `Monolith` [21].
- Hybrid FHE [22]: CHAGHRI [23], HERA [24].

For efficiency in FHE/MPC/ZK applications these primitives must satisfy two novel design criteria: They must be native over a relatively large finite field $\mathbb{F}_q$, where $q \geq 2^{30}$ and often q is prime, and their non-linear components must be representable with a low number of multiplications. The latter condition is often achieved via low-degree univariate permutations.

Unfortunately, the aforementioned investigations into the (c-)Boomerang uniformity hardly yield any results applicable to cryptanalysis of FHE/MPC/ZK-friendly primitives. Henceforth, cryptodesigners would have to work out the (c-)BCT by hand for every novel S-Box. While this is in principle feasible, for example Wang et al. [25] have worked out the 1-Boomerang uniformity of permutation polynomials up to degree 6, such an analysis quickly spans multiple pages for higher degrees. Recently, Steiner [26] addressed this gap in the literature for power permutations x^d of $\mathbb{F}_q$ with $\gcd(d, q) = 1$. For $a, b \in \mathbb{F}_q^\times$ he proved that

$$ {}_c\mathcal{B}_{x^d}(a, b) \leq \begin{cases} d^2, & c^2 \neq 1, \\ d \cdot (d-1), & c = -1, \\ d \cdot (d-2), & c = 1. \end{cases} \tag{3} $$

In this work we extend Equation (3) to permutation polynomials $F \in \mathbb{F}_q[x]$ under minimal structural assumptions on F. In particular, Equation (3) holds for any polynomial with $\gcd\big(\deg(F), q\big) = 1$, see Theorem 12, Proposition 16 and Theorem 18.

1.1 Techniques to Prove the Main Result

On a high level Steiner's proof of Equation (3) proceeds in two steps.

(1) Prove that one of the c-Boomerang polynomials in Equation (2) is irreducible over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$, and verify that the other polynomial is not a multiple of the irreducible one.

(2) Homogenize the polynomials to interpret them as plane curves over $\mathbb{P}^2_{\overline{\mathbb{F}_q}}$, and estimate the intersection number with Bézout's theorem.

For permutation monomials x^d one c-Boomerang polynomial becomes $f_1(x, z) = z^d - c \cdot x^d - b$, where $z = x+y$. Interpreting f_1 as univariate polynomial in $\mathbb{F}_q[x]\big[z\big]$ one can prove its irreducibility via Eisenstein's criterion (if $\gcd(d, q) = 1$), see [26, Lemma 3.3]. Unfortunately, this argument does not generalize to arbitrary permutation polynomials F since it crucially relies on the fact that one can rewrite $f_1(x, z) = z^d - (x - \alpha) \cdot g(x)$, where $\alpha \in \mathbb{F}_q$ is such that $c \cdot \alpha^d = -b$ and $g(\alpha) \neq 0$.

We resolve this problem for the 1-Boomerang uniformity via the Newton polytope method due to Gao [27]. Let $f = \sum_{c_i \neq 0} c_i \cdot x_1^{d_{i_1}} \cdots x_n^{d_{i_n}} \in k[x_1, \ldots, x_n]$ be a polynomial, where k is a

field. For all non-zero coefficients c_i we now collect the exponent vectors $\{\mathbf{d}_i\}_i$ and interpret them as vectors in $\mathbb{R}^n$. The convex closure of $\{\mathbf{d}_i\}_i$ is called the Newton polytope $\mathcal{N}_f$ of f. In particular, for $f, g \in K[x_1, \ldots, x_n]$ one has $\mathcal{N}_{f \cdot g} = \mathcal{N}_f + \mathcal{N}_g$ [27, §2]. Conversely, if the Newton polytope of f cannot be rewritten as sum of polytopes (with positive integer vertices), then f is absolutely irreducible over k.

The Newton polytope of $F(x+y) - F(x) - b$, where $b \neq 0$, turns out to be a triangle, and if $\gcd\left(\deg\left(F\right), q\right) = 1$ then the triangle is integrally indecomposable, see Proposition 11. This yields the generalization of Equation (3) for $c = 1$.

Unfortunately, for $c \neq 1$ the polytope method is not applicable because the c-Boomerang polynomials have too much symmetry. We resolve this problem with Gröbner basis techniques. Let $f \in k[x_1, \ldots, x_n]$ be a polynomial, then we can rewrite it as sum of homogeneous polynomials $f = f_d + f_{d-1} + \ldots + f_0$. In particular, f_d is called the homogeneous highest degree component of f. The highest degree components of the c-Boomerang polynomials admit relatively simple bivariate ideals. By computing the degree reverse lexicographic (DRL) Gröbner basis of the highest degree component ideal, we can already estimate the number of solutions for the c-Boomerang polynomials, which henceforth yields the other two cases of Equation (3), see Proposition 16 and Proposition 17.

Moreover, with Gröbner bases of c-BCT polynomial systems we can construct tight examples for Equation (3).

1.2 Structure of the Paper

In Section 2 we introduce the mathematical preliminaries required of this work. In Section 3 we prove our 1-Boomerang uniformity bounds via geometric methods, and Section 4 we investigate the arithmetic of c-Boomerang polynomial systems to prove the other two cases. In Section 5 we construct tight examples for our bounds. We finish this paper with a short discussion in Section 6.

2 Preliminaries

Let k be a field, then we denote with $\bar{k}$ the algebraic closure of k. We denote the multiplicative group of a field with $k^\times = k \setminus \{0\}$. For $q \in \mathbb{Z}$ a prime power we denote the finite field with q many elements as $\mathbb{F}_q$. Elements of a vector space $\mathbf{a} \in k^n$ are denoted with small bold letters.

Let $f \in k[x_1, \ldots, x_n]$ be a non-zero polynomial, and let x_0 be a new variable. We denote the homogenization of f with respect to x_0 as

$$f^{\text{hom}}(x_0, \ldots, x_n) = x_0^{\deg(f)} \cdot f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in k[x_0, \ldots, x_n]. \tag{4}$$

Conversely, let $F \in k[x_0, \ldots, x_n]$ be homogeneous, then its dehomogenization with respect to x_0 is denoted as

$$F^{\text{deh}}(x_1, \ldots, x_n) = F(1, x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]. \tag{5}$$

For a commutative ring with unity R, an ideal $I \subset R$ is an additive subgroup which is multiplicatively closed. For $I \subset R$ an ideal, its radical is defined as $\sqrt{I} = \{f \in R \mid \exists n \geq 1 \colon f^n \in I\}$. It is well-known that the radical is also an ideal.

2.1 c-Boomerang Uniformity

First, we formally recall the c-Boomerang Connectivity Table and the c-Boomerang uniformity.

Definition 1 (c-Boomerang Uniformity, [6, Remark 1]). *Let $\mathbb{F}_q$ be a finite field, let $c \in \mathbb{F}_q^\times$, and let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a function.*

(1) Let $a, b \in \mathbb{F}_q$. The entry of the c-Boomerang Connectivity Table (c-BCT) of F at (a, b) is defined as

$$ {}_c\mathcal{B}_F(a,b) = \left| \left\{ (x,y) \in \mathbb{F}_q^2 \;\middle|\; \begin{array}{c} F(x+y) - c \cdot F(x) = b \\ c \cdot F(x+y+a) - F(x+a) = c \cdot b \end{array} \right\} \right|. $$

(2) The c-Boomerang uniformity of F is defined as

$$ \beta_{F,c} = \max_{a,b \in \mathbb{F}_q^\times} {}_c\mathcal{B}_F(a,b). $$

Note that Stănică originally defined the c-BCT only for permutations [6, Definition 3] as

$$ {}_c\mathcal{B}_F(a,b) = \left| \left\{ x \in \mathbb{F}_q \mid F^{-1}\left(c^{-1} \cdot F(x+a) + b\right) - F^{-1}\left(c \cdot F(x) + b\right) = a \right\} \right|, \tag{6} $$

which coincides for $c = 1$ with the original definition of the BCT [5, Definition 3.1]. By [6, Theorem 4] Definition 1 (1) and Equation (6) are equivalent for permutations, and in our context it is more convenient to work with Definition 1 (1).

2.2 Plane Curves

For a commutative ring R, the set of prime ideals $\operatorname{Spec}(R) = \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ prime ideal}\}$ is called the spectrum of R. It is well-known that $\operatorname{Spec}(R)$ can be equipped with the Zariski topology, see for example [28, §2.1]. A locally ringed space $(X, \mathcal{O}_X)$ is a topological space X together with a sheaf of commutative rings $\mathcal{O}_X$ on X. If a locally ringed space $(X, \mathcal{O}_X)$ is isomorphic to some $\left(\operatorname{Spec}(R), \mathcal{O}_{\operatorname{Spec}(R)}\right)$, where R is a commutative ring, then $(X, \mathcal{O}_X)$ is called an affine scheme. A scheme $(X, \mathcal{O}_X)$ is a locally ringed space which can be covered by open affine schemes $X = \bigcup_i U_i$, i.e. $\left(U_i = \operatorname{Spec}(R_i), \mathcal{O}_X|_{U_i}\right)$. The dimension of a scheme $(X, \mathcal{O}_X)$ is defined to be the dimension of its underlying topological space X. For a scheme $(X, \mathcal{O}_X)$, if the sheaf $\mathcal{O}_X$ is clear from context we just write X for the scheme. For a general introduction into the scheme-theoretic formulation of algebraic geometry we refer the reader to [28].

For a ring R the n-dimensional affine space $\mathbb{A}_R^n$ is defined to be the scheme $\operatorname{Spec}\left(R[x_1, \ldots, x_n]\right)$, and for an ideal $I \subset R[x_1, \ldots, x_n]$ the scheme $\mathcal{V}(I) = \operatorname{Spec}\left(R[x_1, \ldots, x_n]/I\right)$ is called (affine) vanishing scheme of I. As scheme, the n-dimensional projective space $\mathbb{P}_R^n$ over R is obtained by gluing $n+1$ copies of the affine space $\mathbb{A}_R^n$, see [28, §3.6]. Let $R[X_0, \ldots, X_n]$ be graded via the degree, and let $I \subset R[X_0, \ldots, X_n]$ be a homogeneous ideal. Analogously to the construction of $\mathbb{P}_R^n$, one can construct a scheme $\mathcal{V}_+(I)$ together with a closed immersion $\iota : \mathcal{V}_+(I) \to \mathbb{P}_R^n$. Therefore, $\mathcal{V}_+(I)$ is called the projective vanishing scheme of I, see [28, §3.7].

Let k be a field, let $k \subset K$ be a field extension, and let X be a k-scheme. The K-valued points of X are given by $X(K) = \operatorname{Hom}_k\left(\operatorname{Spec}(K), X\right)$. For affine/projective vanishing schemes the K-valued points have an elementary interpretation.

Example 2. Let k be a field, let $k \subset K$ be a field extension, let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let $J \subset k[X_0, \ldots, X_n]$ be a homogeneous ideal.

(1) $\mathbb{A}_k^n(k) = k^n$ [28, Example 4.2]. I.e., the k-valued points correspond to the elementary definition of the affine space.

(2) $\mathcal{V}(I)(k) = \{\mathbf{x} \in \mathbb{A}_k^n(k) \mid \forall f \in I \colon f(\mathbf{x}) = 0\}$ [28, Example 4.3]. I.e., the k-valued points correspond to the elementary definition of the affine variety.

(3) $\mathbb{P}_k^n(k)$ is given by points $\mathbf{x} \in \left(k^{n+1} \setminus \{\mathbf{0}\}\right)/\sim$ with the equivalence relation $\mathbf{x} \sim \mathbf{y} \Leftrightarrow \exists a \in k^\times : \mathbf{x} = a \cdot \mathbf{y}$ [28, Exercise 4.6]. I.e., the k-valued points correspond to the elementary definition of the projective space.

(4) $\mathcal{V}_+(I)(K) = \{\mathbf{x} \in \mathbb{P}_K^n(K) \mid \forall f \in J \colon f(\mathbf{x}) = 0\}$ [28, Example 5.3]. I.e., the K-valued points correspond to the elementary definition of the projective variety.

Let k be a field, and let $F, G \in k[X_0, X_1, X_2]$. The vanishing scheme $\mathcal{V}_+(F) \subset \mathbb{P}_k^n$ is also called *plane curve*. It is well-known that the scheme-theoretic intersection of two plane curves [28, Example 4.38] is given by

$$\mathcal{V}_+(F) \cap \mathcal{V}_+(G) = \mathcal{V}_+(F, G) \subset \mathbb{P}_k^2. \tag{7}$$

Counting the number of points in intersections of vanishing schemes is a standard problem in algebraic geometry. Next, we recall the intersection number tailored for plane curves.

Definition 3 ([28, Definition 5.60])**.** *Let k be a field, and let $C, D \subset \mathbb{P}_k^2$ be two plane curves such that $Z := C \cap D$ is a k-scheme of dimension 0. Then we call $i(C, D) := \dim_k\left(\Gamma(Z, \mathcal{O}_Z)\right)$ the intersection number of C and D. For $z \in Z$ we call $i_z(C, D) := \dim_k(\mathcal{O}_{Z,z})$ the intersection number of C and D at z.*

From the definition it is easily verified that

$$i(C, D) = \sum_{z \in C \cap D} i_z(C, D). \tag{8}$$

Bézout's famous theorem states that the intersection number of two plane curves together with their multiplicities is equal to the product of their degrees.

Theorem 4 (Bézout's Theorem, [28, Theorem 5.61])**.** *Let k be a field, and let $C = \mathcal{V}_+(F)$ and $D = \mathcal{V}_+(G)$ be plane curves in $\mathbb{P}_k^2$ given by polynomials without a common factor. Then*

$$i(C, D) = \deg(F) \cdot \deg(G).$$

In particular, the intersection $C \cap D$ is non-empty and consists of a finite number of closed points.

2.3 Polytope Method

It is well-known that polynomial rings over fields $P = k[x_1, \ldots, x_n]$ are unique factorization domains. A polynomial $f \in P$ is called *irreducible* if for every factorization $f = g \cdot h$, with $g, h \in P$, one hast that either $g \in k^\times$ or $h \in k^\times$. Additionally, an irreducible polynomial $f \in P$ is called *absolutely irreducible* if it remains irreducible over every algebraic field extension $k \subset K$.

A standard algorithmic problem in commutative algebra is the decomposition of f into its irreducible factors with multiplicities. However, it is often useful to decide whether f is irreducible or not without explicit factorization of f. For the latter purpose, mathematicians developed various irreducibility criteria. In this paper, we work with Gao's polytope method [27].

Let $S \subset \mathbb{R}^n$ be a subset, then S is called *convex* if for any two points $\mathbf{x}, \mathbf{y} \in S$ the line segment for $\mathbf{x}$ to $\mathbf{y}$ is also contained in S, i.e.

$$\forall 0 \leq t \leq 1 \colon \mathbf{x} + t \cdot (\mathbf{y} - \mathbf{x}) = (1 - t) \cdot \mathbf{x} + t \cdot \mathbf{y} \in S. \tag{9}$$

The smallest convex set of $\mathbb{R}^n$ which contains S is called the *convex closure* $\operatorname{conv}(S)$ of S. The following identity is well-known

$$\operatorname{conv}(S) = \left\{ \sum_{i=1}^{n} t_i \cdot \mathbf{a}_i \;\middle|\; \mathbf{a}_i \in S,\ t_i \geq 0,\ \sum_{i=1}^{n} t_i = 1 \right\}. \tag{10}$$

For a finite set $S = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ we also denote the convex closure as $\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$. The convex closure of a finite set S is also called *polytope*, and a point of a polytope is called *vertex* if it is not on the line segment of any other two points of the polytope. With Equation (10) it is easy to verify that a polytope is equal to the convex closure of its vertices.

Returning to polynomials, any $f \in k[x_1, \ldots, x_n]$ can be expressed as finite sum $f = \sum_i c_i \cdot x_1^{d_{i_1}} \cdots x_n^{d_{i_n}}$, where $c_i \in k^\times$. Naturally, we can consider the exponent vectors $\mathbf{d}_i = (d_{i_1}, \ldots, d_{i_n})^\intercal \subset \mathbb{Z}^n_{\geq 0}$ as elements of $\mathbb{R}^n$. The *Newton polytope* $\mathcal{N}_f$ of f is then defined to be the convex closure $\operatorname{conv}\left(\{\mathbf{d}_i\}_i\right)$ of f's exponent vectors.

For two sets $A, B \subset \mathbb{R}^n$, their *Minkowski sum* is defined as $A + B = \{a + b \mid a \in A,\ b \in B\}$. Let $f, g, h \in k[x_1, \ldots, x_n]$ be such that $f = g \cdot h$, fundamental to Gao's irreducibility criterion is the identity [27, Lemma 2.1]

$$\mathcal{N}_f = \mathcal{N}_g + \mathcal{N}_h. \tag{11}$$

A point $\mathbf{x} \in \mathbb{R}^n$ is called *integral* if $\mathbf{x} \in \mathbb{Z}^n$, and a polytope is called integral if all its vertices are integral. An integral polytope C is called *integrally decomposable* if it can be written as Minkowski sum $C = A + B$ with A and B integral polytopes too. Otherwise, C is called *integrally indecomposable*. Finally, we can express Gao's irreducibility criterion.

Theorem 5 (Gao's Irreducibility Criterion, [27, §2])**.** *Let k be a field, and let $f \in k[x_1, \ldots, x_n]$ be a non-zero polynomial not divisible by any x_i. If the Newton polytope of f is integrally indecomposable, then f is absolutely irreducible.*

In this paper we will encounter triangles, i.e. polytopes generated by three distinct points $\langle \mathbf{x}, \mathbf{y}, \mathbf{z} \rangle \subset \mathbb{R}^n$. For integral triangles, Gao has fully characterized being integrally indecomposable. Let $\mathbf{a} = (a_1, \ldots, a_n)^\intercal, \mathbf{b} \in \mathbb{Z}^n$, for ease of writing we abbreviate $\gcd(\mathbf{a}) = \gcd(a_1, \ldots, a_n)$, and analogously for $\gcd(\mathbf{a}, \mathbf{b})$.

Corollary 6 ([27, Corollary 4.5])**.** *Let $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}^n$ be three points not all on one line. Then the triangle $\langle \mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2 \rangle$ is integrally indecomposable if and only if*

$$\gcd(\mathbf{v}_0 - \mathbf{v}_1, \mathbf{v}_0 - \mathbf{v}_2) = 1.$$

2.4 Triangles

For our study of triangle Newton polytopes we also need some basic properties of triangles, which can be proven with elementary Euclidean geometry. For an introduction to Euclidean geometry we refer the reader to [29].

By mirroring, any triangle $\Delta = \mathbf{ABC} \subset \mathbb{R}^2$ can be extended to a parallelogram $P = \mathbf{ABDC} \subset \mathbb{R}^2$, see Figure 1. Let $\mathbf{a} = \mathbf{B} - \mathbf{A} = \begin{pmatrix} a_x \\ a_y \end{pmatrix}$ and $\mathbf{b} = \mathbf{C} - \mathbf{A} = \begin{pmatrix} b_x \\ b_y \end{pmatrix}$ denote the edge vectors spanning the parallelogram, then the area of P is given by the determinant

$$\mathcal{A}_P = \left| \det \begin{pmatrix} a_x & b_x \\ a_y & b_y \end{pmatrix} \right| \qquad \Longrightarrow \qquad \mathcal{A}_\Delta = \frac{1}{2} \cdot \left| \det \begin{pmatrix} a_x & b_x \\ a_y & b_y \end{pmatrix} \right|. \tag{12}$$

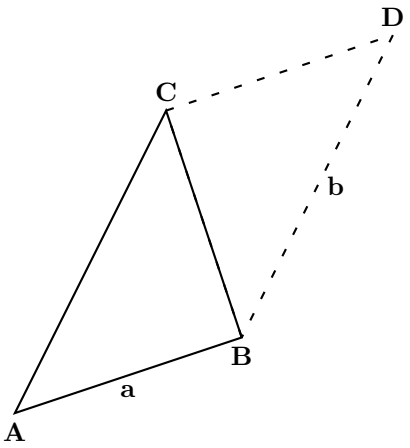
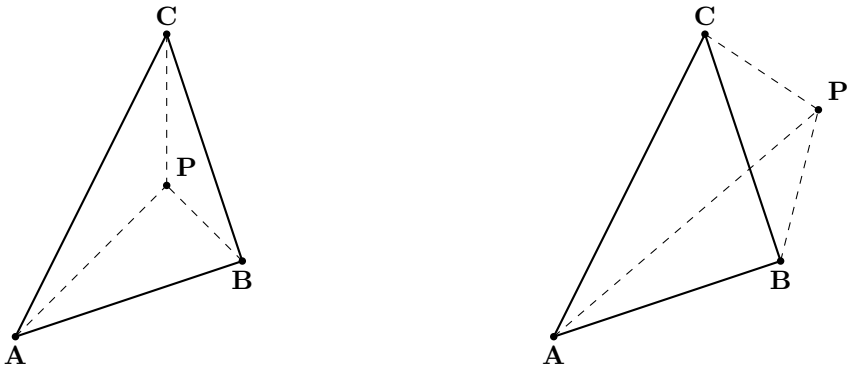


Figure 1: Mirrored triangle.

Let $\Delta = \mathbf{ABC} \subset \mathbb{R}^2$ be a triangle, and let $\mathbf{P} \in \mathbb{R}^2$ be a point not lying on one of the edges **BA**, **CB** or **AC**. To decide whether **P** lies within the triangle Δ, we consider the three triangles $\Delta_1 = \mathbf{ABP}$, $\Delta_2 = \mathbf{APC}$ and $\Delta_3 = \mathbf{PBC}$. If the area identity $\mathcal{A}_\Delta = \mathcal{A}_{\Delta_1} + \mathcal{A}_{\Delta_2} + \mathcal{A}_{\Delta_3}$ is satisfied, then **P** indeed lies within Δ, otherwise the identity is not satisfied. This property is illustrated in Figure 2.



(a) Inside. **(b)** Outside.

Figure 2: Illustration of a point lying inside or outside a triangle.

2.5 Gröbner Bases

Gröbner bases are a tool to solve computational problems of ideals $I \subset k[x_1, \ldots, x_n]$ like the membership problem, computation of the dimension or computation of the set of zeros. For the definition of Gröbner bases we first have to introduce term orders on $k[x_1, \ldots, x_n]$.

Definition 7 (Term Order, [30, Chapter 2 §2 Definition 1])**.** *Let k be a field, a term order $>$ on $k[x_1, \ldots, x_n] = k[\mathbf{x}]$ is a relation $>$ on $\mathbb{Z}^n_{\geq 0}$, or equivalently, a relation on the set of monomials $\mathbf{x}^\mathbf{a} = \prod_{i=1}^n x_i^{a_i}$, $\mathbf{a} \in \mathbb{Z}^n_{\geq 0}$, satisfying:*

(i) $>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$.

(ii) *If* $\mathbf{a} > \mathbf{b}$ *and* $\mathbf{c} \in \mathbb{Z}^n_{\geq 0}$, *then* $\mathbf{a} + \mathbf{c} > \mathbf{b} + \mathbf{c}$.

(iii) $>$ *is a well-ordering on* $\mathbb{Z}^n_{\geq 0}$. *I.e., every non-empty subset of* $\mathbb{Z}^n_{\geq 0}$ *has a smallest element under* $>$.

In this paper we work with the *lexicographic* (LEX) and the *degree reverse lexicographic* (DRL) term order:

- $\mathbf{a} >_{LEX} \mathbf{b}$ if the leftmost non-zero entry of $\mathbf{a} - \mathbf{b}$ is positive.
- $\mathbf{a} >_{DRL} \mathbf{b}$ if either $\sum_{i=1}^n a_i > \sum_{i=1}^n b_i$, or $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ and the rightmost non-zero entry of $\mathbf{a} - \mathbf{b}$ is negative.

Let $f \in P = k[x_1, \ldots, x_n]$ be a non-zero polynomial, and let $>$ be a term order on P. The largest monomial present in f is called the *$>$-leading monomial*, and the coefficient of the largest monomial is called *$>$-leading coefficient*. We denote them as $\mathrm{LM}_>(f)$ and $\mathrm{LC}_>(f)$ respectively. Now we can recall the definition of a Gröbner basis.

Definition 8 (Gröbner Basis, [30, Chapter 2 §5 Definition 5]). *Let k be a field, let $I \subset P = k[x_1, \ldots, x_n]$ be a non-zero ideal, and let $>$ be a term order on P. A finite subset $\mathcal{G} \subset I$ is said to be a $>$-Gröbner basis if*

$$\big(\mathrm{LM}_>(g) \;\big|\; g \in \mathcal{G}\big) = \big(\mathrm{LM}_>(f) \;\big|\; f \in I\big).$$

Next we describe a computational criterion to detect Gröbner bases due to Buchberger. Let $f, g \in P = k[x_1, \ldots, x_n]$ and let $>$ be a term order on P. The *S-polynomial* of f and g is defined as

$$S_>(f,g) = \frac{\mathrm{lcm}\big(\mathrm{LM}_>(f), \mathrm{LM}_>(g)\big)}{\mathrm{LC}_>(f)} \cdot f - \frac{\mathrm{lcm}\big(\mathrm{LM}_>(f), \mathrm{LM}_>(g)\big)}{\mathrm{LC}_>(g)} \cdot g. \tag{13}$$

Buchberger's criterion requires the multivariate polynomial division algorithm, readers can find its description in [30, Chapter 2 §3].

Theorem 9 (Buchberger's Criterion, [30, Chapter 2 §6 Theorem 6]). *Let k be a field, let $I \subset P = k[x_1 \ldots, x_n]$, and let $>$ be a term order on P. Then a basis $\mathcal{G} = \{g_1, \ldots, g_m\} \subset I$ of I is a $>$-Gröbner basis if and only if for all pairs $i \neq j$, the remainder on division of $S_>(g_i, g_j)$ by $\mathcal{G}$ (listed in some order) is zero.*

This criterion yields a very simple algorithm to compute Gröbner basis. For the input set $\mathcal{F}$, compute the remainders of all possible S-polynomials with respect to $\mathcal{F}$. If a remainder is non-zero, add it to $\mathcal{F}$ and repeat until Buchberger's criterion is satisfied. This procedure is known as Buchberger's algorithm [31].

Let $>$ be a term order on $P = k[x_1, \ldots, x_n]$. An ideal $I \subset P = k[x_1, \ldots, x_n]$ is zero-dimensional, i.e. $\dim(P/I) = 0$ if and only if for every $1 \leq i \leq n$ there exists $f \in I$ and $d_i \in \mathbb{Z}_{\geq 1}$ such that $\mathrm{LM}_>(f) = x_i^{d_i}$, see [30, Chapter 5 §3 Theorem 6] and [32, Theorem 5.11]. In particular, let $d = \dim_k(P/I) < \infty$ denote the k-vector space dimension of the quotient ring, then [30, Chapter 5 §3 Proposition 7]

$$\big|\mathcal{V}(I)(k)\big| = \big|\{\mathbf{x} \in k^n \;|\; \forall f \in I \colon f(\mathbf{x}) = 0\}\big| \leq d, \tag{14}$$

with equality if k is algebraically closed and I is radical.

For a general introduction into the theory of Gröbner bases we refer the reader to [30, 33, 34].

3 Irreducibility of 1-Boomerang Polynomials

We now prove our first main result of this paper, the absolute irreducibility of polynomials $f(x) - f(y) + a$, which yields the 1-Boomerang uniformity bound by Bézout's theorem.

As preparation, we recall that irreducibility of a polynomial is invariant under linear variable transformations.

Lemma 10. *Let k be a field, let $f \in k[\mathbf{x}] = k[x_1, \ldots, x_n]$, and let $\mathbf{M} \in \mathbb{F}_q^{n \times n}$ be such that $\det(\mathbf{M}) \neq 0$. Then $f(\mathbf{x})$ is irreducible if and only if $f(\mathbf{Mx})$ is irreducible*

Proof. Let $\mathbf{y} = \mathbf{Mx}$, then we have a ring isomorphism $\phi : k[\mathbf{x}] \to k[\mathbf{y}]$. Now assume that $\phi(f) = \phi(f_1) \cdot \phi(f_2)$, since ϕ is an isomorphism we have $f = f_1 \cdot f_2$. If f is irreducible, then either $f_1 \in k^\times$ or $f_2 \in k^\times$. Since $\phi(k^\times) = k^\times$ this implies that $\phi(f)$ is irreducible too. The other direction follows identical. □

The irreducibility proof is an application of the polytope method.

Proposition 11. *Let k be a field of characteristic $p \in \mathbb{Z}_{\geq 0}$.*

(1) Let $d \in \mathbb{Z}_{\geq 2}$, and let $i_1, i_2 \in \mathbb{Z}_{\geq 1}$. Then the polytope

$$\left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ d-1 \end{pmatrix}, \begin{pmatrix} d \\ 0 \end{pmatrix}, \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} \right\rangle_{2 \leq i_1 + i_2 \leq d} = \left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ d-1 \end{pmatrix}, \begin{pmatrix} d \\ 0 \end{pmatrix} \right\rangle \subset \mathbb{R}^2$$

is an integrally indecomposable triangle.

(2) Let $f \in k[X]$ with $d = \deg(f) > 0$, and let $a \in k^\times$. If $p > 0$, then assume in addition that $\gcd(d, p) = 1$. Then

$$F = f(x) - f(y) + a \in k[x, y]$$

is absolutely irreducible over k.

Proof. We first consider the polynomial F. Let $f = \sum_{i=1}^{d} a_i \cdot x^i$,[1] then

$$\begin{aligned} F(x+y, y) &= f(x+y) - f(y) + a \\ &= \left(\sum_{i=1}^{d} a_i \cdot (x+y)^i \right) - f(y) + a \\ &= \left(f(x) + \sum_{i=2}^{d} a_i \cdot \sum_{j=1}^{i-1} \binom{i}{j} \cdot x^j \cdot y^{i-j} + f(y) \right) - f(y) + a \\ &= f(x) + \sum_{i=2}^{d} a_i \cdot \sum_{j=1}^{i-1} \binom{i}{j} \cdot x^j \cdot y^{i-j} + a. \end{aligned}$$

In particular, in characteristic $p > 0$ we have by assumption for $i = d$ and $j = 1$ that $\binom{i}{j} = \binom{d}{1} = d \not\equiv 0 \mod p$, i.e. the monomial $x \cdot y^{d-1}$ is present in $F(x+y, y)$. Therefore, all exponents which can be present in $F(x+y, y)$ are contained in the set

$$\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} j \\ 0 \end{pmatrix}, \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} \right\}_{\substack{1 \leq j \leq d, \\ 2 \leq i_1 + i_2 \leq d}}.$$

[1] Since the constant term of f is canceled in F we can without loss of generality assume that $f(0) = 0$.

Recall that for a convex set $\mathcal{C} \subset \mathbb{R}^n$ and a point $\mathbf{p} \in \mathcal{C}$ we have for the convex closure that $\langle \mathcal{C}, \mathbf{p} \rangle = \mathcal{C}$. Thus,

$$\left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} j \\ 0 \end{pmatrix}, \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} \right\rangle_{\substack{1 \le j \le d, \\ 2 \le i_1 + i_2 \le d}} = \left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ d-1 \end{pmatrix}, \begin{pmatrix} d \\ 0 \end{pmatrix}, \begin{pmatrix} i_1 \\ i_2 \end{pmatrix} \right\rangle_{2 \le i_1 + i_2 \le d}. \tag{15}$$

(The points $(j, 0)^\intercal$ trivially lie on the line from $(0, 0)^\intercal$ to $(d, 0)^\intercal$.) Now we want to prove that this polytope is indeed a triangle. In Figure 3 we provide an illustration of the polytope from the assertion.

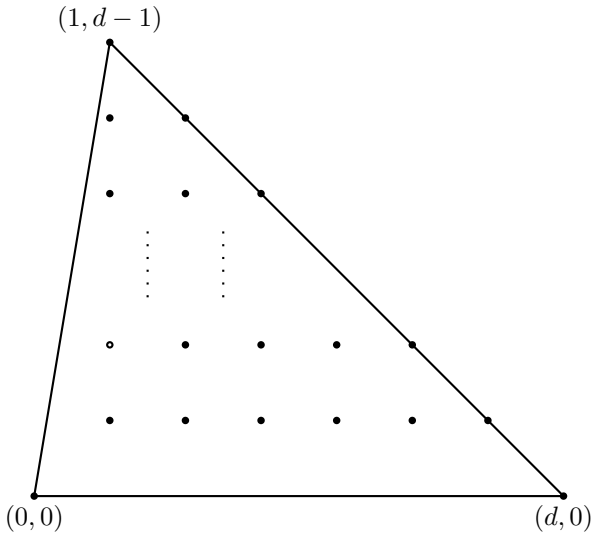


Figure 3: Illustration of the triangle.

For ease of notation, let $\Delta = \left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ d-1 \end{pmatrix}, \begin{pmatrix} d \\ 0 \end{pmatrix} \right\rangle$. It is clear that every point $\mathbf{p} = (i_1, i_2)^\intercal$ with $i_1 + i_2 = d$ lies on the line from $(1, d-1)^\intercal$ to $(d, 0)^\intercal$, so they are indeed in the triangle. For the other points $\mathbf{p} = (i_1, i_2)^\intercal$ with $2 \le i_1 + i_2 < d$, we consider the triangles

$$\Delta_1 = \left\langle \mathbf{p}, \begin{pmatrix} 1 \\ d-1 \end{pmatrix}, \begin{pmatrix} d \\ 0 \end{pmatrix} \right\rangle, \qquad \Delta_2 = \left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \mathbf{p}, \begin{pmatrix} d \\ 0 \end{pmatrix} \right\rangle, \qquad \Delta_3 = \left\langle \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ d-1 \end{pmatrix}, \mathbf{p} \right\rangle,$$

and verify whether we have the area identity

$$\mathcal{A}_\Delta = \mathcal{A}_{\Delta_1} + \mathcal{A}_{\Delta_2} + \mathcal{A}_{\Delta_3},$$

or not, see Section 2.4 and Figure 2. Let $k = i_1 + i_2$, then we have the triangle areas, see Section 2.4,

$$\begin{aligned} \mathcal{A}_\Delta &= \frac{1}{2} \cdot \left| \det \begin{pmatrix} d & 0 \\ 1 & d-1 \end{pmatrix} \right| &&= \frac{d \cdot (d-1)}{2}, \\ \mathcal{A}_{\Delta_1} &= \frac{1}{2} \cdot \left| \det \begin{pmatrix} d-i_1 & -i_2 \\ 1-i_1 & d-1-i_2 \end{pmatrix} \right| &&= \frac{|d \cdot (d-1) - k \cdot (d-1)|}{2}, \end{aligned}$$

$$\mathcal{A}_{\Delta_2} = \frac{1}{2} \cdot \left| \det \begin{pmatrix} d & 0 \\ i_1 & i_2 \end{pmatrix} \right| = \frac{i_2 \cdot d}{2},$$
$$\mathcal{A}_{\Delta_3} = \frac{1}{2} \cdot \left| \det \begin{pmatrix} i_1 & i_2 \\ 1 & d-1 \end{pmatrix} \right| = \frac{|i_1 \cdot d - k|}{2}.$$

Since $i_1 \geq 1$ and $k \leq d$ we can drop the absolute values in $\mathcal{A}_{\Delta_1}$ and $\mathcal{A}_{\Delta_3}$. Now we observe that

$$\frac{d \cdot (d-1) - k \cdot (d-1)}{2} + \frac{i_2 \cdot d}{2} + \frac{i_1 \cdot d - k}{2} = \frac{d \cdot (d-1)}{2}.$$

So, all the points from the assertion indeed are inside the triangle Δ or its boundary, hence the convex closure from Equation (15) is indeed a triangle.

For integral indecomposability of Δ, note that

$$\gcd\left(\begin{pmatrix} 1 \\ d-1 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} d \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right) = \gcd(0, 1, d-1, d) = 1,$$

and the claim follows from Corollary 6. This proves (1).

Returning to $F(x+y, y)$, due to the assumption that $\gcd(d, p) = 1$ if $p > 0$ the monomials $1, x^d, x \cdot y^{d-1}$ have non-zero coefficients. Combining all our previous observation we conclude that Δ is exactly the Newton polytope of $F(x+y, y)$. So, absolute irreducibility of $F(x+y, y)$ follows from Theorem 5, and absolute irreducibility of $F(x, y)$ follows from Lemma 10. This proves (2). □

Now we apply Bézout's theorem to the 1-Boomerang polynomials.

Theorem 12. *Let $\mathbb{F}_q$ be a finite field, let $f \in \mathbb{F}_q[x]$ with $d = \deg(f) > 0$ be a polynomial such that $\gcd(d, q) = 1$, and let $a, b \in \mathbb{F}_q^\times$. Then ${}_1\mathcal{B}_f(a, b) \leq d \cdot (d-2)$.*

Proof. Let $a, b \in \mathbb{F}_q^\times$. We consider the 1-Boomerang equations with the substitution $z = x + y$

$$F_1 = f(z) - f(x) - b,$$
$$F_2 = f(z+a) - f(x+a) - b,$$

as polynomials in $\mathbb{F}_q[x, z]$. By Proposition 11 F_1 is absolutely irreducible. Now let us consider

$$F_2 - F_1 = \big(f(z+a) - f(z)\big) - \big(f(x+a) - f(x)\big).$$

Then, all points $z = x$ are roots of this polynomial. In particular, via elementary methods, see e.g. [26, Lemma 3.5] we can prove that $F_2 - F_1 = (z - x) \cdot G_2$, where $G_2 \in \mathbb{F}_q[x, z]$. Let us substitute $z = x$ into F_1 which yields $b = 0$. Since $b \in \mathbb{F}_q^\times$ the boomerang equations do not have a symmetric solution. Therefore, we can replace $F_2 - F_1$ by $G_2 = \frac{F_2 - F_1}{z - x}$. Note that $\deg(G_2) \leq d - 2$.

Now we homogenize F_1 and G_2 with respect to a new variable X_0 and consider $F_1^{\text{hom}}, G_2^{\text{hom}} \in \mathbb{F}_q[X_0, X, Z]$ as plane curves in $\mathbb{P}^2_{\mathbb{F}_q}$. Since factorization is invariant under homogenization [34, Proposition 4.3.2] F_1^{hom} is still irreducible. Since $\deg\left(G_2^{\text{hom}}\right) = \deg(G_2) < \deg(F_1) = \deg\left(F_1^{\text{hom}}\right)$ these curves cannot have a common irreducible component. So, by Bézout's theorem (Theorem 4) we have

$$i\Big(\mathcal{V}_+\big(F_1^{\text{hom}}\big), \mathcal{V}_+\big(G_2^{\text{hom}}\big)\Big) = \deg(F_1) \cdot \deg(G_2) = d \cdot (d-2)$$

$$= \sum_{z \in \mathcal{V}_+(F_1^{\hom}) \cap \mathcal{V}_+(G_2^{\hom})} \dim_k \left(\mathcal{O}_{\mathcal{V}_+(F_1^{\hom}) \cap \mathcal{V}_+(G_2^{\hom}), z} \right)$$
$$\geq \sum_{z \in \mathcal{V}_+(F_1^{\hom}) \cap \mathcal{V}_+(G_2^{\hom})} 1,$$

where the inequality follows from $\overline{\mathbb{F}_q} \hookrightarrow \mathcal{O}_{\mathcal{V}_+(F_1^{\hom}) \cap \mathcal{V}_+(G_2^{\hom}), z}$. It follows from zero-dimensionality [28, Lemmma 5.59] that all points in $\mathcal{V}_+\left(F_1^{\hom}\right) \cap \mathcal{V}_+\left(G_2^{\hom}\right)$ [28, Lemmma 5.59] are closed. Now recall the $\overline{\mathbb{F}_q}$-valued points of the intersection, see Example 2,

$$\begin{aligned}\left(\mathcal{V}_+(F_1^{\hom}) \cap \mathcal{V}_+(G_2^{\hom})\right)(\overline{\mathbb{F}_q}) &= \mathcal{V}_+\left(F_1^{\hom}, G_2^{\hom}\right)(\overline{\mathbb{F}_q}) \\ &= \left\{ \mathbf{x} \in \mathbb{P}^2_{\overline{\mathbb{F}_q}}(\overline{\mathbb{F}_q}) \;\middle|\; F_1^{\hom}(\mathbf{x}) = G_2^{\hom}(\mathbf{x}) = 0 \right\}.\end{aligned}$$

Over an algebraically closed field k the k-valued points are in one to one bijection with the closed points [28, Corollary 3.36]. Therefore,

$$\left| \left\{ \mathbf{x} \in \mathbb{P}^2_{\overline{\mathbb{F}_q}}(\overline{\mathbb{F}_q}) \;\middle|\; F_1^{\hom}(\mathbf{x}) = G_2^{\hom}(\mathbf{x}) = 0 \right\} \right| \leq d \cdot (d-2).$$

Finally, let $U_0 = \left\{ (X_0, X, Z) \in \mathbb{P}^2_{\overline{\mathbb{F}_q}} \;\middle|\; X_0 \neq 0 \right\}$, then we have [30, Chapter 8 §2 Proposition 6]

$$\left\{ \mathbf{x} \in \mathbb{P}^2_{\overline{\mathbb{F}_q}}(\overline{\mathbb{F}_q}) \;\middle|\; F_1^{\hom}(\mathbf{x}) = G_2^{\hom}(\mathbf{x}) = 0 \right\} \cap U_0 = \left\{ \mathbf{x} \in \overline{\mathbb{F}_q}^2 \;\middle|\; F_1(\mathbf{x}) = G_2(\mathbf{x}) = 0 \right\},$$

so also the number of affine solutions of the 1-Boomerang polynomials is bounded by $d \cdot (d-2)$. □

In characteristic 2 the bound can be slightly improved.

Corollary 13. *Let $\mathbb{F}_q$ be a finite field of characteristic 2, let $f \in \mathbb{F}_q[X]$ with $d = \deg(f) > 0$ be a polynomial such that $\gcd(d, q) = 1$, and let $a, b \in \mathbb{F}_q^\times$. Then ${}_1\mathcal{B}_f(a, b) \leq d \cdot (d-2) - 1$.*

Proof. By Theorem 12 we have that ${}_1\mathcal{B}_f(a, b) \leq d \cdot (d-2)$. Since $\gcd(d, q) = 1$ we have that $d \cdot (d-2)$ is odd. On the other hand, in characteristic 2 the boomerang equations, see Definition 1, are symmetric. Thus, the number of solutions must be even, and the bound from Theorem 12 is not attainable. □

With Proposition 11 we can also prove a special case for the -1-Boomerang uniformity.

Corollary 14. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $f \in \mathbb{F}_q[X]$ with $d = \deg(f) > 0$ be a polynomial such that*

(i) $\gcd(d, q) = 1$, *and*

(ii) $f(-x) = -f(x)$.

Let $a, b \in \mathbb{F}_q^\times$. Then

(1) *$f(x + y) + f(x) + b$ is absolutely irreducible.*

(2) ${}_{-1}\mathcal{B}_f(a, b) \leq d \cdot (d-1)$.

Proof. We consider the -1-Boomerang equations with the substitution $z = x + y$

$$F_1 = f(z) + f(x) - b,$$
$$F_2 = f(z + a) + f(x + a) - b.$$

Next we perform the substitution $x = -\hat{x}$, then

$$F_1 = f(z) - f(\hat{x}) - b,$$

and by Lemma 10 and Proposition 11 this polynomial is absolutely irreducible.

Since $\deg(F_2 - F_1) \leq (d-1) < d = \deg(F_1)$, these polynomials cannot share an irreducible component after homogenization. Now we can apply Bézout's theorem analog to Theorem 12 to yield the bound. □

4 Arithmetic of c-Boomerang Polynomial Systems

For $c = -1$ the c-Boomerang equations are symmetric, see Definition 1. In particular, their Newton polytopes are symmetric triangles. However, the GCD criterion for triangle indecomposability (Corollary 6) requires a non-symmetry in the triangle.[2] Therefore, as an alternative approach to derive c-Boomerang uniformity bounds we study in this section the arithmetic of c-Boomerang polynomial systems.

Recall that for $f \in k[x_1, \ldots, x_n]$ we denote the highest homogeneous component of f with f^{top}. Then for $\mathcal{F} \subset k[x_1, \ldots, x_n]$ a finite system of polynomials, we denote $\mathcal{F}^{\text{top}} = \{f^{\text{top}}\}_{f \in \mathcal{F}}$. Central to our arithmetic investigations are the following properties of the highest degree components ideal $(\mathcal{F}^{\text{top}})$.

Lemma 15. *Let k be a field, let $\mathcal{F} \subset P = k[x_1, \ldots, x_n]$ be a finite system of polynomials, and let $d = \dim_k\left(P/(\mathcal{F}^{\text{top}})\right)$. Then*

(1) $\left(\text{LM}_{DRL}(f) \;\middle|\; f \in (\mathcal{F}^{\text{top}})\right) \subset \left(\text{LM}_{DRL}(f) \;\middle|\; f \in (\mathcal{F})\right)$.

(2) $\dim_k\left(P/(\mathcal{F})\right) \leq d$.

Proof. Let $h \in (\mathcal{F}^{\text{top}})$ be non-zero, then we can express it as

$$h = \sum_{f \in \mathcal{F}^{\text{top}}} g_f \cdot f^{\text{top}},$$

where $g_f \in P$ is homogeneous and if it is non-zero then $\deg(g_f) = \deg(h) - \deg(f)$. We can lift h to an element $\hat{h} \in (\mathcal{F})$ via

$$\hat{h} = \sum_{f \in \mathcal{F}} g_f \cdot f,$$

and by homogeneity of the g_f's we have that $\deg\left(\hat{h}\right) = \deg(h)$ and $\text{LM}_{DRL}\left(\hat{h}\right) = \text{LM}_{DRL}(h)$. This proves (1).

For (2), if $d = \infty$ the inequality is trivial, otherwise we recall that one possible k-vector space basis of $P/(\mathcal{F})$ is given by all monomials not contained in $\left(\text{LM}_{DRL}(f) \;\middle|\; f \in (\mathcal{F})\right)$ [30, Chapter 5 §3 Proposition 4]. Via the inclusion from (1) we then have $\left|P \setminus \left\{\text{LM}_{DRL}(f) \;\middle|\; f \in (\mathcal{F})\right\}\right| \leq \left|P \setminus \left\{\text{LM}_{DRL}(f) \;\middle|\; f \in (\mathcal{F}^{\text{top}})\right\}\right| = d$. □

[2] A bit more precise, the Newton polytope of $F = f(x) + f(y) + a$, where $d = \deg(f)$ and $f(0) = 0$, is given by $\left\langle \mathbf{0}, (d,0)^\intercal, (0,d)^\intercal \right\rangle$, and $\gcd\left((d,0)^\intercal, (0,d)^\intercal\right) = 1$.

Thus, if we can construct $x_i^{d_i} \in \left(\mathrm{LM}_{DRL}(f) \mid f \in (\mathcal{F}^{\mathrm{top}})\right)$ for every variable x_i, then we have immediately established the following two properties:

(1) Zero-dimensionality of $(\mathcal{F}^{\mathrm{top}})$ and $(\mathcal{F})$, see [30, Chapter 5 §3 Theorem 6] and [32, Theorem 5.11].

(2) $\left|\mathcal{V}(\mathcal{F})(k)\right| = \dim_k\left(P/(\mathcal{F})\right) \leq \dim_k\left(P/\left(\mathcal{F}^{\mathrm{top}}\right)\right) \leq \prod_{i=1}^{n} d_i$, see [30, Chapter 5 §3 Proposition 7].

The highest degree components of the c-Boomerang polynomials are relatively simple bivariate polynomials, which allows construction of their DRL Gröbner bases by hand.

4.1 $c^2 \neq 1$

We start with the simplest case $c^2 \neq 1$, for which we can trivially compute a DRL Gröbner basis of the c-Boomerang polynomials.

Proposition 16. *Let $\mathbb{F}_q$ be a finite field, let $f \in \mathbb{F}_q[X]$ with $d = \deg(f)$, let $c \in \mathbb{F}_q^\times$ be such that $c^2 \neq 1$, let $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$, and let $F_1, F_2 \in \mathbb{F}_q[x, z]$ be the c-Boomerang polynomials of (a, b). Then*

(1) $\left\{F_1, c^{-1} \cdot F_2 - F_1\right\}$ is a DRL Gröbner basis of (F_1, F_2) for $z >_{DRL} x$.

(2) ${}_c\mathcal{B}_f(a, b) \leq d^2$.

Proof. Starting from the c-Boomerang polynomials

$$\begin{aligned} F_1 &= f(z) - c \cdot f(x) - b, \\ F_2 &= c \cdot f(z + a) - f(x + a) - b, \end{aligned}$$

we equip $\mathbb{F}_q[x, z]$ with the DRL term order $z >_{DRL} x$. Then $\mathrm{LM}_{DRL}(F_1) = z^d$. Moreover,

$$c^{-1} \cdot F_2 - F_1 = \left(f(z - a) - f(z)\right) + c^{-1} \cdot \left(f(x + a) - c^2 \cdot f(x)\right) - b \cdot \left(1 - c^{-1}\right).$$

Note that this polynomial does not have the monomial z^d, but since $c^2 \neq 1$ it has the monomial x^d. If a set of polynomials has pairwise coprime leading monomials, then it is already a Gröbner basis, see [30, Chapter 2 §9 Theorem 3, Proposition 4]. Moreover, the number of monomials not contained in $(x^d, z^d) \in \mathbb{F}_q[x, z]$ is exactly d^2. By [30, Chapter 5 §3 Proposition 7] this proves the claim. □

4.2 $c = -1$

Next we investigate the highest degree components for $c = -1$.

Proposition 17. *Let k be a field of characteristic $p \neq 2$, let $d \in \mathbb{Z}_{\geq 2}$, let $I = \left(x^d + y^d, x^{d-1} + y^{d-1}\right) \subset k[x, y]$, and let $x >_{DRL} y$. Then*

(1) I has the DRL Gröbner basis

$$\mathcal{G} = \{g_1, g_2, g_3\} = \left\{x^{d-1} + y^{d-1}, x \cdot y^{d-1} - y^d, y^{2 \cdot d - 2}\right\}.$$

(2) $\dim_k\left(k[x, y]/I\right) = d \cdot (d - 1)$.

Proof. For (1), first we show that indeed $\mathcal{G} \subset I$. We have that

$$g_2 = S_{DRL}\left(x^{d-1} + y^{d-1}, x^d + y^d\right) = x \cdot y^{d-1} - y^d.$$

We claim that

$$y^{d-1} \cdot \left(x^{d-1} + y^{d-1}\right) \equiv 2 \cdot y^{2 \cdot d-2} \mod \left(x \cdot y^{d-1} - y^d\right). \tag{16}$$

To prove this assertion we perform inductive division by remainder with respect to DRL on the terms on the left-hand side Equation (16). In the first step of the division algorithm we reduce

$$x^{d-1} \cdot y^{d-1} = x^{d-2} \cdot \left(x \cdot y^{d-1}\right) \equiv x^{d-2} \cdot y^d \mod \left(x \cdot y^{d-1} - y^d\right).$$

Next we have to reduce

$$x^{d-2} \cdot y^d = x^{d-3} \cdot y \cdot \left(x \cdot y^{d-1}\right) \equiv x^{d-3} \cdot y^{d+1} \mod \left(x \cdot y^{d-1} - y^d\right).$$

Per induction, in the i^{th} iteration we have to reduce

$$x^{d-i} \cdot y^{d+i-2} = x^{d-i-1} \cdot y^{i-1} \cdot \left(x \cdot y^{d-1}\right) \equiv x^{d-i-1} \cdot y^{d+i-1} \mod \left(x \cdot y^{d-1} - y^d\right).$$

This procedure will eventually terminate in $i = d-1$ where we arrive at the term $y^{2 \cdot d-2}$. Since $y^{2 \cdot d-2}$ is also present in the left-hand side of Equation (16) we obtain the final remainder $2 \cdot y^{2 \cdot d-1} \neq 0$, since we work in characteristic $p \neq 2$. Note that this division process can also be expressed as

$$y^{d-1} \cdot \left(x^{d-1} + y^{d-1}\right) - \left(x \cdot y^{d-1} - y^d\right) \cdot \left(\sum_{i=0}^{d-2} x^{d-2-i} \cdot y^i\right) = 2 \cdot y^{2 \cdot d-2}.$$

It also immediately follows that $(\mathcal{G}) = I$. Next we verify Buchberger's criterion (Theorem 9):

- $S_{DRL}(g_1, g_3)$ can be ignored due to coprimality of the leading monomials, see [30, Chapter 2 §9 Theorem 3, Proposition 4].
- The remainder of $S_{DRL}(g_1, g_2)$ with respect to $\mathcal{G}$ corresponds exactly to the polynomial division of Equation (16), i.e. $S_{DRL}(g_1, g_2) \equiv 2 \cdot g_3 \equiv 0 \mod (\mathcal{G})$.
- For the last pair

$$S_{DRL}(g_2, g_3) = y^{d-1} \cdot \left(x \cdot y^{d-1} - y^d\right) - x \cdot y^{2 \cdot d-2} = -y^{2 \cdot d-1} \equiv 0 \mod \left(y^{2 \cdot d-2}\right).$$

So, $\mathcal{G}$ is indeed the DRL Gröbner basis of I.

For (2), by [30, Chapter 5 §3 Proposition 7] we have to count the monomials not contained in $\left(x^{d-1}, x \cdot y^{d-1}, y^{2 \cdot d-2}\right) \subset k[x, y]$. There are

- $d-2$ monomials $x, \ldots, x^{d-2}$,
- $(d-2)^2$ monomials $x^k \cdot y^l$, where $1 \leq k, l \leq d-2$, and
- $2 \cdot (d-1) - 1$ monomials $y, \ldots, y^{2 \cdot d-3}$.

So, incorporating the constant monomial 1 we have the k-vector space dimension $1 + d - 2 + (d-2)^2 + 2 \cdot (d-1) - 1 = d \cdot (d-1)$. □

The homogeneous ideal from Proposition 17 is exactly the highest degree components ideal for $c = -1$ after an obvious preprocessing step.

Theorem 18. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, let $f \in \mathbb{F}_q[x]$ with $d = \deg(f)$ be such that $\gcd(d, q) = 1$, and let $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Then ${}_{-1}\mathcal{B}_f(a, b) \leq d \cdot (d-1)$.*

Proof. Let $f = \sum_{i=0}^{d} a_i \cdot x^i$. We consider the -1-Boomerang equations with the substitution $z = x + y$

$$\begin{aligned} F_1 &= f(z) + f(x) - b, \\ F_2 &= f(z+a) + f(x+a) - b, \end{aligned}$$

as polynomials in $\mathbb{F}_q[x, z]$. Observe that

$$\Delta_a f(x) = f(x+a) - f(x) = \sum_{i=0}^{d} a_i \cdot \left((x+a)^i - x^i\right) = a_d \cdot d \cdot a \cdot x^{d-1} + \ldots,$$

and since by assumption $\gcd(d, q) = 1$ this is a polynomial of degree $d-1$. Now let

$$G_2 = F_2 - F_1 = \Delta_a f(z) + \Delta_a f(x).$$

Then $\left(F_1^{\text{top}}, G_2^{\text{top}}\right) = \left(z^d + x^d, z^{d-1} + x^{d-1}\right)$, and the claim follows from Proposition 17. □

4.3 $c = 1$

For completeness, we also reinvestigate the case $c = 1$.

Proposition 19. *Let k be a field of characteristic p, let $d \in \mathbb{Z}_{\geq 3}$, let $I = \left(x^d - y^d, \sum_{i+j=d-2} x^i \cdot y^j\right) \subset k[x, y]$, and let $x >_{DRL} y$. If $p > 0$, then assume in addition that $\gcd(d-1, p) = 1$. Then*

(1) I has the DRL Gröbner basis

$$\mathcal{G} = \{g_1, g_2, g_3\} = \left\{ \sum_{i+j=d-2} x^i \cdot y^j, x \cdot y^{d-1} - y^d, y^{2 \cdot d - 3} \right\}.$$

(2) $\dim_k\left(k[x, y]/I\right) = d \cdot (d-2)$.

Proof. For (1), note that

$$(x - y) \cdot \left(\sum_{i+j=d-2} x^i \cdot y^j \right) = x^{d-1} - y^{d-1},$$

see for example the proof of [26, Lemma 3.5], and

$$g_2 = S_{DRL}\left(x^d - y^d, x^{d-1} - y^{d-1}\right) = x \cdot y^{d-1} - y^d.$$

We claim that

$$y^{d-1} \cdot \left(\sum_{i+j=d-2} x^i \cdot y^j \right) \equiv (d-1) \cdot y^{2 \cdot d - 2} \mod \left(x \cdot y^{d-1} - y^d\right). \tag{17}$$

To prove this assertion we perform inductive division by remainder with respect to DRL on the terms on the left-hand side Equation (17). In the first step of the division algorithm we reduce

$$x^{d-2} \cdot y^{d-1} = x^{d-3} \cdot \left(x \cdot y^{d-1}\right) \equiv x^{d-3} \cdot y^d \mod \left(x \cdot y^{d-1} - y^d\right).$$

Since $y^{d-1} \cdot \left(x^{d-3} \cdot y\right) = x^{d-3} \cdot y^d$ is also present in the left-hand side of Equation (17), in the second step we have to reduce

$$2 \cdot x^{d-3} \cdot y^d = 2 \cdot x^{d-4} \cdot y \cdot \left(x \cdot y^{d-1}\right) \equiv 2 \cdot x^{d-4} \cdot y^{d+1} \mod \left(x \cdot y^{d-1} - y^d\right).$$

Per induction, in the i^{th} iteration we have to reduce

$$i \cdot x^{d-i-1} \cdot y^{d+i-2} = i \cdot x^{d-i-2} \cdot y^{i-1} \cdot \left(x \cdot y^{d-1}\right) \equiv i \cdot x^{d-i-2} \cdot y^{d+i-1} \mod \left(x \cdot y^{d-1} - y^d\right).$$

This procedure will eventually terminate in $i = d-2$ where we arrive at the term $(d-2) \cdot y^{2 \cdot d-3}$. Since $y^{2 \cdot d-3}$ is also present in the left-hand side of Equation (17) we obtain the final remainder $(d-1) \cdot y^{2 \cdot d-3}$. If $p > 0$, then by assumption $d - 1 \not\equiv 0 \mod p$, so the final remainder is indeed non-zero which implies $\mathcal{G} \subset I$. Note that this division process can also be expressed as

$$y^{d-1} \cdot \left(\sum_{i+j=d-2} x^i \cdot y^j\right) - \left(x \cdot y^{d-1} - y^d\right) \cdot \left(\sum_{i=0}^{d-3} (i+1) \cdot x^{d-3-i} \cdot y^i\right) = (d-1) \cdot y^{2 \cdot d-3}.$$

It also immediately follows that $(\mathcal{G}) = I$. Next we verify Buchberger's criterion (Theorem 9):

- $S_{DRL}(g_1, g_3)$ can be ignored due to coprimality of the leading monomials, see [30, Chapter 2 §9 Theorem 3, Proposition 4].
- $S_{DRL}(g_1, g_2)$ corresponds exactly to the first step in the polynomial division of Equation (17), therefore $S_{DRL}(g_1, g_2) \equiv (d-1) \cdot g_3 \equiv 0 \mod (\mathcal{G})$.
- For the last pair

$$S_{DRL}(g_2, g_3) = y^{d-2} \cdot \left(x \cdot y^{d-1} - y^d\right) - x \cdot y^{2 \cdot d-3} = -y^{2 \cdot d-2} \equiv 0 \mod \left(y^{2 \cdot d-3}\right).$$

So, $\mathcal{G}$ is indeed the DRL Gröbner basis of I.

For (2), by [30, Chapter 5 §3 Proposition 7] we have to count the monomials not contained in $\left(x^{d-2}, x \cdot y^{d-1}, y^{2 \cdot d-3}\right) \subset k[x, y]$. There are

- $d-3$ monomials $x, \ldots, x^{d-3}$,
- $(d-3) \cdot (d-2)$ monomials $x^k \cdot y^l$, where $1 \leq k \leq d-3$ and $1 \leq l \leq d-2$, and
- $2 \cdot d - 4$ monomials $y, \ldots, y^{2 \cdot d-4}$.

So, incorporating the constant monomial 1 we have the k-vector space dimension $1 + d - 3 + (d-3) \cdot (d-2) + 2 \cdot d - 4 = d \cdot (d-2)$. □

If we apply Proposition 19 to the 1-Boomerang polynomials we obtain a slightly more restricted bound than Theorem 12.

Corollary 20. *Let $\mathbb{F}_q$ be a finite field, and let $f \in \mathbb{F}_q[x]$ with $d = \deg(f)$ be such that $\gcd(d, q) = \gcd(d-1, q) = 1$, and let $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Then ${}_1\mathcal{B}_f(a, b) \leq d \cdot (d-2)$.*

Proof. Let $f = \sum_{i=0}^{d} a_i \cdot x^i$. We consider the -1-Boomerang equations with the substitution $z = x + y$

$$F_1 = f(z) - f(x) - b,$$
$$F_2 = f(z+a) - f(x+a) - b,$$

as polynomials in $\mathbb{F}_q[x, z]$. Observe that

$$\Delta_a f(x) = f(x+a) - f(x) = \sum_{i=0}^{d} a_i \cdot \left((x+a)^i - x^i\right) = a_d \cdot d \cdot a \cdot x^{d-1} + \ldots,$$

and since by assumption $\gcd(d, q) = 1$ this is a polynomial of degree $d-1$. Now let

$$\tilde{F}_2 = F_2 - F_1 = \Delta_a f(z) - \Delta_a f(x).$$

As discussed in the proof of Theorem 12, $(z - x) \mid \tilde{F}_2$ and we can replace it by $G_2 = \frac{\tilde{F}_2}{z-x}$, which has degree $d-2$. In particular, $(F_1^{\text{top}}, G_2^{\text{top}}) = \left(z^d - x^d, \sum_{i+j=d-2} z^i \cdot x^j\right)$, this again follows from the proof of [26, Lemma 3.5], and we obtain the inequality via Proposition 19. □

On the other hand, the improved bound in characteristic 2 from Corollary 13 is not covered by Proposition 19 respectively Corollary 20.

5 Constructing Tight Examples

With the aid of `SageMath` [35] we now construct tight examples for Theorem 12, Corollary 13, Proposition 16 and Theorem 18. For $f \in \mathbb{F}_q[X]$ and $c \in \mathbb{F}_q^\times$, our tight examples are found via the following procedure:

(1) Pick $a, b \in \mathbb{F}_q^\times$ and set up the c-Boomerang polynomials $F_1, F_2 \in \mathbb{F}_q[x, z]$.

(2) Compute the DRL Gröbner basis of (F_1, F_2) for $z >_{DRL} x$.
Compute $D = \dim_{\mathbb{F}_q}\left(\mathbb{F}_q[x, z]/(F_1, F_2)\right)$. If D is less than the expected bound, pick different (a, b).

(3) Compute the LEX Gröbner basis for $z >_{LEX} x$ via term order conversion [36].
If the LEX basis is not of the form $\{z - g_1(x), g_2(x)\}$, pick different (a, b).

(4) Factor $g_2(x)$.
If every factor has multiplicity we pass to an appropriate field extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ such that g_2 decomposes into distinct linear factors. Otherwise, pick different (a, b).

In Algorithm 1 we provide the `SageMath` function for generation of the c-Boomerang polynomials.

Algorithm 1 Construction of c-Boomerang Polynomials.

```
def c_boomerang_polynomials(f,     # A polynomial in Fq [X].
                            a,     # An element in Fq.
                            b,     # An element in Fq.
                            c=1,   # An element in Fq.
                           ):
    P = PolynomialRing(f.parent().base_ring(), ["z", "x"], order="degrevlex")
    z = P.gens()[0]
    x = P.gens()[1]
    F_1 = f(z) - c * f(x) - b
    F_2 = c * f(z + a) - f(x + a) - c * b
    return [F_1, F_2]
```

5.1 A Short Excursion on Dickson Polynomials

Dickson polynomials have numerous applications in the study of finite fields. In particular, they provide a generic way to instantiate permutation polynomials. All our tight examples in this section are instantiations of Dickson polynomials.

Definition 21 ([37]). *Let $\mathbb{F}_q$ be a finite field, let $n \in \mathbb{Z}_{\geq 0}$, and let $a \in \mathbb{F}_q$. The n^{th} Dickson polynomial (of the first kind) is defined as*

$$D_n(X,a) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \cdot \binom{n-i}{i} \cdot (-a)^i \cdot X^{n-2\cdot i} \in \mathbb{F}_q[X].$$

The following properties of Dickson polynomials are well-known:

- $D_n(X,0) = X^n$.
- For $n \geq 2$ they satisfy the recurrence relation [37, Lemma 2.3]

$$D_n(X,a) = X \cdot D_{n-1}(X,a) - a \cdot D_{n-2}(X,a). \tag{18}$$

- $D_n(X,a)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd\left(n, q^2-1\right) = 1$ [38, 7.16. Theorem].
- They satisfy a commutation relation under composition [37, Lemma 2.6]

$$D_{m\cdot n}(X,a) = D_m\left(D_n(X,a), a^n\right) = D_n\left(D_m(X,a), a^m\right). \tag{19}$$

- They satisfy [37, Lemma 2.3]

$$b^n \cdot D_n(X,a) = D_n(b\cdot X, b^2 \cdot a). \tag{20}$$

- For p the characteristic of $\mathbb{F}_q$ they satisfy [37, Lemma 2.3]

$$D_{p\cdot n}(X,a) = \left(D_n(X,a)\right)^p. \tag{21}$$

- If $2 \mid d$, then all terms on $D_d(X,a)$ have even degree.
- If $2 \nmid d$, then all terms on $D_d(X,a)$ have odd degree.

Thus, given a Dickson polynomial of degree $p^k \cdot d$ where $p \nmid d$ and $d > 1$, then we can reduce the c-Boomerang equations of $D_{p^k \cdot d}(X, a)$ to c-Boomerang equations of $D_d(X, a)$ via an application of a linearized permutation monomial. Thus, we can always apply Theorems 12 and 18 to estimate the ± 1-Boomerang uniformity of Dickson polynomials.

In Algorithm 2 we provide the `SageMath` function for generation of Dickson polynomials.

Algorithm 2 Construction of n^{th} Dickson polynomial.

```
def dickson_polynomial(n, # Degree of the Dickson polynomial.
                       a, # Coefficient of the Dickson polynomial,
                          # must be an element of a SageMath ring.
                       ):
    ring = a.parent()
    P = PolynomialRing(ring, 'X')
    X = P.gen()
    p = 0
    for i in range(0, floor(n / 2) + 1):
        p += Integer((n / (n - i)) * binomial(n - i, i)) * ring(-a)**i * X**(n - 2 * i)
    return p
```

The c-BCT of Dickson polynomials satisfies the following relation.

Lemma 22. *Let $\mathbb{F}_q$ be a finite field, let $n \in \mathbb{Z}_{\geq 1}$, let $\alpha, \beta \in \mathbb{F}_q^\times$, and let $\gamma = \frac{\beta}{\alpha}$. If either*

(i) α and β are squares, or

(ii) α and β are non-squares,

then ${}_c\mathcal{B}_{D_n(x,\alpha)}(a, b) = {}_c\mathcal{B}_{D_n(x,\beta)}\left(\gamma^{\frac{1}{2}} \cdot a, \gamma^{\frac{n}{2}} \cdot b\right)$. In particular, $\beta_{D_n(x,\alpha),c} = \beta_{D_n(x,\beta),c}$.

Proof.

- If α and β are squares, then γ is one too.
- If α and β are non-squares, then γ is a square.[3]

Therefore, in either case we can utilize Equation (20) as follows

$$\gamma^{\frac{n}{2}} \cdot D_n(x, \alpha) = D_n\left(\gamma^{\frac{1}{2}} \cdot x, \gamma \cdot \alpha\right) = D_n\left(\gamma^{\frac{1}{2}} \cdot x, \beta\right).$$

From Definition 1 it then follows that ${}_c\mathcal{B}_{D_n(x,\alpha)}(a, b) = {}_c\mathcal{B}_{D_n(x,\beta)}\left(\gamma^{\frac{1}{2}} \cdot a, \gamma^{\frac{n}{2}} \cdot b\right)$. □

This lemma has an interesting consequence. If we consider $\left\{\alpha, \beta_{D_n(x,\alpha),c}\right\}_{\alpha \in \mathbb{F}_q}$ as table, then we can have at most three distinct entries for $\beta_{D_n(x,\alpha),c}$. Namely, one entry for $\alpha = 0$, one for α square and one for α non-square.

Example 23. Let $q = 11$, then we have the following c-Boomerang uniformities for $D_7(X, \alpha)$.

Table 1: c-Boomerang uniformities of $D_7(X, \alpha)$ over $\mathbb{F}_{11}$.

	$\beta_{D_7(x,\alpha),c}$									
c	1	2	3	4	5	6	7	8	9	10
$\alpha = 0$	3	5	2	2	2	5	2	2	2	4
α square	6	3	4	4	3	3	5	5	3	6
α non-square	5	5	3	3	3	5	3	3	3	4

[3] A very elegant argument for the product of non-squares in $\mathbb{F}_q$ being square which does not require cyclicity of $\mathbb{F}_q^\times$ was given in https://math.stackexchange.com/a/1938451/696633.

The `SageMath` code to compute the c-Boomerang uniformities of Dickson polynomials over $\mathbb{F}_{11}$ can be found in Algorithm 3.

5.2 Examples for $c = 1$

First, we present a tight example for Theorem 12 in odd characteristic.

Example 24. Let $q = 11$, let $f = X^7$, and let $a = 1$ and $b = 3$. Then, the DRL Gröbner basis $z >_{DRL} x$ of the boomerang equations is

$$\begin{aligned}
g_1 = \; & x^{11} + 4z^4x^5 + 8x^9 - z^4x^4 + 8z^3x^5 + 3x^8 - z^4x^3 + 4z^3x^4 + 8z^2x^5 + 7x^7 + 5z^4x^2 - z^3x^3 + 7z^2x^4 \\
& + 4zx^5 + 5x^6 + 5z^4x + z^3x^2 + 6z^2x^3 + zx^4 - x^5 + 8z^4 + 7z^3x + 5z^2x^2 + 6zx^3 + 5x^4 + 8z^3 - z^2x \\
& + 7zx^2 + 3x^3 + 7z^2 + 9zx + 8x^2 + 6z + 3x + 1, \\
g_2 = \; & zx^6 - x^7 + 3zx^5 + 8x^6 + 7z^4x + 7z^3x^2 + 7z^2x^3 + zx^4 + 9x^5 + 9z^4 - z^3x - z^2x^2 + 4zx^3 + 6x^4 + 3z^3 \\
& + 2z^2x + 5zx^2 + 9x^3 - z^2 + 3zx + 4x^2 + 2z + 7x + 4, \\
g_3 = \; & z^5 + z^4x + z^3x^2 + z^2x^3 + zx^4 + x^5 + 3z^4 + 3z^3x + 3z^2x^2 + 3zx^3 + 3x^4 + 5z^3 + 5z^2x \\
& + 5zx^2 + 5x^3 + 5z^2 + 5zx + 5x^2 + 3z + 3x + 1,
\end{aligned}$$

and the LEX Gröbner basis with $z >_{LEX} x$ is

$$\begin{aligned}
h_1 = \; & z + 5x^{34} + 4x^{33} + 5x^{32} + 4x^{31} + 6x^{30} + x^{29} + 8x^{28} + x^{26} + 9x^{25} + 4x^{23} - x^{22} + 7x^{20} - x^{19} + 4x^{18} \\
& + 6x^{17} - x^{16} + x^{15} + 9x^{14} + 4x^{13} + 9x^{12} + 2x^{11} + 3x^{10} + 2x^9 + 8x^8 + 6x^7 + 6x^6 + 2x^5 + 5x^3 + 4x^2 \\
& + 6x + 6, \\
h_2 = \; & (x+7)\cdot(x+10)\cdot(x+4)\cdot(x^2+6x+1)\cdot(x^2+8x+3)\cdot(x^4-x^3+8x^2+4x+3) \\
& \cdot(x^4-x^3+9x^2+7)\cdot(x^{20}+x^{19}+x^{18}-x^{17}+4x^{16}+3x^{15}+6x^{14}-x^{13}+x^{12}+5x^{11}+9x^{10}+x^9 \\
& + 7x^8 + 3x^6 + 7x^5 + 8x^4 + 6x^3 + 7x^2 + 9x + 3).
\end{aligned}$$

Therefore, over the finite field of size q^{20} the univariate LEX polynomial will decompose into linear factors and Theorem 12 becomes tight. Also, note that $\gcd\left(7, q^{20} - 1\right) = 1$. The code for this example is provided in Algorithm 4.

Next we present a tight example for Corollary 13 in characteristic 2.

Example 25. Let $\mathbb{F}_{2^4}(g) \cong \mathbb{F}_2[Y]/\left(Y^4 + Y + 1\right)$, let $f = D_{11}(X, 1)$, and let $a = g^2 + 1$ and $b = g^3 + g^2 + g$. Then, the LEX Gröbner basis $z >_{LEX} x$ of the boomerang equations is of the form

$$\begin{aligned}
h_1 &= z + \tilde{h}_{1,1}(x), \\
h_2 &= \prod_{i=1}^{9} \tilde{h}_{2,i}(x),
\end{aligned}$$

where $\deg\left(\tilde{h}_{1,1}\right) = 96$, $\deg\left(\tilde{h}_{2,1}\right) = \ldots = \deg\left(\tilde{h}_{2,3}\right) = 2$, $\deg\left(\tilde{h}_{2,4}\right) = \deg\left(\tilde{h}_{2,5}\right) = 4$, $\deg\left(\tilde{h}_{2,6}\right) = \deg\left(\tilde{h}_{2,7}\right) = 14$ and $\deg\left(\tilde{h}_{2,8}\right) = \deg\left(\tilde{h}_{2,9}\right) = 28$. So, $\dim_{\mathbb{F}_q}(h_1, h_2) = 98 = 11 \cdot (11 - 2) - 1$, and over the finite field of size $q^{14} = 2^{56}$ the univariate LEX polynomial decomposes into linear factors and Corollary 13 becomes tight. Also, note that $\gcd\left(11, 2^{2\cdot 56} - 1\right) = 1$. The code for this example is provided in Algorithm 5.

5.3 Examples for $c = -1$

Now we present a tight example for Theorem 18 in odd characteristic.

Example 26. Let $q = 257$, let $f = X^5$, and let $a = 1$ and $b = 48$. Then, the DRL Gröbner basis $z >_{DRL} x$ of the -1-Boomerang equations is

$$\begin{aligned}
g_1 &= x^8 + 4x^7 + 2z^3x^3 + 8x^6 + 3z^3x^2 + 3z^2x^3 + 10x^5 + 156z^3x + 158z^2x^2 + 156zx^3 + 214x^4 + 182z^3 \\
&\quad + 235z^2x + 235zx^2 + 84x^3 + 158z^2 + 210zx + 57x^2 + 55z + 4x + 120, \\
g_2 &= zx^4 - x^5 + 2zx^3 + 255x^4 + 255z^3 + 2zx^2 + 253x^3 + 254z^2 + zx + 253x^2 + 204z + 255x + 150, \\
g_3 &= z^4 + x^4 + 2z^3 + 2x^3 + 2z^2 + 2x^2 + z + x + 206,
\end{aligned}$$

and the LEX Gröbner basis with $z >_{LEX} x$ is

$$\begin{aligned}
h_1 &= z + 198x^{19} + 33x^{18} + 165x^{17} + 77x^{16} + 45x^{15} + 84x^{14} + 122x^{13} + 190x^{12} + 166x^{11} + 12x^{10} + 79x^9 \\
&\quad + 2x^8 + 120x^7 + 100x^6 + 239x^5 + 61x^4 + 96x^3 + 59x^2 + 141x + 161, \\
h_2 &= (x^2 + 9x + 3) \cdot (x^2 + 25x + 255) \cdot (x^2 + 33x + 132) \cdot (x^2 + 50x + 24) \cdot (x^2 + 55x + 197) \\
&\quad \cdot (x^2 + 95x + 164) \cdot (x^2 + 134x + 125) \cdot (x^2 + 192x + 35) \cdot (x^2 + 219x + 41) \cdot (x^2 + 226x + 86).
\end{aligned}$$

Therefore, over the finite field of size q^2 the univariate LEX polynomial will decompose into linear factors and Theorem 18 becomes tight. Also, note that $\gcd(5, q-1) = \gcd\left(5, q^2-1\right) = 1$. The code for this example is provided in Algorithm 6.

We also provide a Dickson polynomial example.

Example 27. Let $p = 89$, let $f = D_7(X, 1)$, and let $a = 1$ and $b = 17$. Then, the DRL Gröbner basis $z >_{DRL} x$ of the -1-Boomerang equations is

$$\begin{aligned}
g_1 &= x^{12} + 6x^{11} + 2z^5x^5 + 9x^{10} + 5z^5x^4 + 5z^4x^5 + 79x^9 + 15z^4x^4 + 57x^8 + 84z^5x^2 + 5z^4x^3 + 5z^3x^4 \\
&\quad + 84z^2x^5 + 87x^7 + 37z^5x + 24z^4x^2 + 49z^3x^3 + 24z^2x^4 + 37zx^5 + 50x^6 + 11z^5 + 29z^4x + 34z^3x^2 \\
&\quad + 34z^2x^3 + 29zx^4 + 60x^5 + 20z^4 + 10z^3x + 35z^2x^2 + 10zx^3 + x^4 + 12z^3 + 5z^2x + 5zx^2 + 32x^3 \\
&\quad + 34z^2 + 7zx + 25x^2 + 66z + 3x + 24, \\
g_2 &= zx^6 - x^7 + 3zx^5 + 86x^6 + 87z^5 + 87x^5 + 84z^4 + 84zx^3 - zx^2 + x^3 + 5z^2 + 2zx + 3x^2 + 14z \\
&\quad + x + 67, \\
g_3 &= z^6 + x^6 + 3z^5 + 3x^5 + 84z^3 + 84x^3 - z^2 - x^2 + 2z + 2x + 13,
\end{aligned}$$

and the LEX Gröbner basis with $z >_{LEX} x$ is

$$\begin{aligned}
h_1 &= z + 71x^{41} + 86x^{40} + 41x^{39} + 73x^{38} + 82x^{37} + 20x^{36} + 37x^{35} + 30x^{34} + 65x^{33} + 56x^{32} + 51x^{31} + 63x^{30} \\
&\quad + 11x^{29} - x^{28} + 32x^{27} + 25x^{26} + 56x^{25} + 27x^{24} + 24x^{23} + 22x^{22} + 58x^{21} + 25x^{20} + 42x^{19} + 85x^{18} \\
&\quad + 45x^{17} + 59x^{16} + 55x^{15} + 84x^{14} + 37x^{12} + 79x^{11} + 85x^{10} + 71x^9 + 47x^8 + 16x^7 + 49x^6 + 75x^5 \\
&\quad + 66x^4 + 86x^3 + 55x^2 + 77x + 28, \\
h_2 &= (x + 28) \cdot (x + 34) \cdot (x + 73) \cdot (x + 80) \cdot (x + 85) \cdot x \cdot (x + 9) \cdot (x + 60) \cdot (x^2 + 32x + 55) \\
&\quad \cdot (x^2 + 72x + 13) \cdot (x^{10} + 26x^9 + 79x^8 + 63x^7 + 45x^6 + 64x^5 + 15x^4 + 16x^3 + 44x^2 + 11x + 20) \\
&\quad \cdot (x^{10} + 62x^9 + 31x^8 + 3x^7 + 16x^6 + 69x^5 + 84x^4 + 73x^3 + 16x^2 + 50x + 36) \\
&\quad \cdot (x^{10} + 83x^9 + 16x^8 + 30x^7 + 4x^6 + 27x^5 + 6x^4 + 67x^3 + 69x^2 + 65x + 88).
\end{aligned}$$

Therefore, over the finite field of size $q10$ the univariate LEX polynomial will decompose into linear factors and Corollary 14 becomes tight. Also, note that $\gcd\left(7, q^2-1\right) = \gcd\left(7, q^{20}-1\right) = 1$. The code for this example is provided in Algorithm 7.

5.4 Example for $c^2 \neq 1$

Finally, we present an example for Proposition 16.

Example 28. Let $q = 191$, let $f = X^3$, and let $a = 1$ and $b = 125$. Then, the LEX Gröbner basis $z >_{LEX} x$ of the 11-Boomerang equations is

$$h_1 = z + 126x^8 + 110x^7 + 95x^6 + 45x^5 + 65x^4 + 107x^3 + 15x^2 + 181x + 166,$$
$$h_2 = (x+102)\cdot(x+140)\cdot(x+145)\cdot(x+167)\cdot(x+173)\cdot(x+179)\cdot(x+184)\cdot(x+45)\cdot(x+73).$$

Therefore, Proposition 16 is tight for $c = 11$. Also, note that $\gcd(3, q-1) = 1$. The code for this example is provided in Algorithm 8.

6 Discussion

In this paper we have generalized the c-Boomerang uniformity bounds from [26] for permutation monomials (Equation (3)) to arbitrary permutation polynomials. In [26, §5] the monomial bounds were utilized to estimate c-BCTs of permutations over $\mathbb{F}_q^n$ based on the *Generalized Triangular Dynamical System* (GTDS) [39]. Likewise, our bounds can be utilized to generalize the estimations from [26, Theorem 5.5].

In [26, §4] tightness of the ±1-Boomerang uniformity bounds for monomials was investigated with symbolic Gröbner basis computations, and two conjectures for $\left(\mathrm{LM}_{DRL}(f) \;\middle|\; f \in (F_1, F_2)\right) \subset \mathbb{F}_q[x, z]$, where F_1 and F_2 are the ±1-Boomerang polynomials, were proposed [26, Conjecture 4.3, 4.4]. Our investigations into the arithmetic of c-Boomerang polynomial systems (Section 4) answer these conjectures in the affirmative if we have for the degree d that $\gcd(d\cdot(d-1), q) = 1$. In particular, if q is a prime number and $d < q$, the conjectures are true.

Readers might have noticed that most of our examples in Section 5 become tight over relatively large field extension (compared to the base field). Therefore, one might wonder whether it is possible to quantify how small the fraction $\frac{d}{q}$ has to be "on average" so that our bounds from Theorem 12, Proposition 16 and Theorem 18 become tight.

A SageMath Code

Algorithm 3 c-Boomerang uniformities of Dickson polynomials over $\mathbb{F}_{11}$.

```
q = 11
K = GF(q)
sep = 30 * "-"
for c in range(1, q):
    print(sep)
    print("c:", c)
    print("alpha", "\t",
          "a", "\t",
          "b", "\t",
          "beta")
    for alpha in range(0, q):
        f = dickson_polynomial(7, K(alpha))
        a_max = 0
        b_max = 0
        D_max = 0
        for a in range(1, q):
            for b in range(1, q):
                polys = c_boomerang_polynomials(f, a, b, c=c)
                fes = [var**q - var for var in polys[0].parent().gens()]
                I = ideal(polys + fes)
                gb = I.groebner_basis()
                D = len(ideal(gb).normal_basis())
                if D > D_max:
                    a_max = a
                    b_max = b
                    D_max = D
        print(alpha, "\t",
            a_max, "\t",
            b_max, "\t",
            D_max)
```

Algorithm 4 Code for Example 24.

```
q = 11
K = GF(q)
P = PolynomialRing(K, "X")
X = P.gen()
f = X**7
a = 1
b = 3
polys = c_boomerang_polynomials(f, a, b)
I = ideal(polys)
gb = I.groebner_basis()
print("DRL Groebner Basis")
for poly in gb:
    print(poly)
print("")
gb_lex = ideal(gb).transformed_basis(algorithm="fglm")
print("Lexicographic Groebner Basis")
for poly in gb_lex:
    print(poly)
print("")
print("Factorization of Univariate LEX Polynomial")
for fac in gb_lex[-1].factor():
    print(fac)
```

Algorithm 5 Code for Example 25.

```
q = 2**4
Y = polygen(GF(2))
K = GF(q, "g", modulus=Y**4 + Y + 1)
g = K.gen()
f = dickson_polynomial(11, K(1))
a = g^2 + 1
b = g^3 + g^2 + g
polys = c_boomerang_polynomials(f, a, b)
polys = c_boomerang_polynomials(f, a, b)
I = ideal(polys)
gb = I.groebner_basis()

print("DRL Groebner Basis")
for poly in gb:
    print(poly)
print("")
gb_lex = ideal(gb).transformed_basis(algorithm="fglm")
print("Lexicographic Groebner Basis")
for poly in gb_lex:
    print(poly)
print("")
print("Factorization of Univariate LEX Polynomial")
for fac in gb_lex[-1].factor():
    print(fac)
```

Algorithm 6 Code for Example 26.

```
q = 257
K = GF(q)
P = PolynomialRing(K, "X")
X = P.gen()
f = X**5
a = 1
b = 48
polys = c_boomerang_polynomials(f, a, b, c=-1)
I = ideal(polys)
gb = I.groebner_basis()
print("DRL Groebner Basis")
for poly in gb:
    print(poly)
print("")
gb_lex = ideal(gb).transformed_basis(algorithm="fglm")
print("Lexicographic Groebner Basis")
for poly in gb_lex:
    print(poly)
print("")
print("Factorization of Univariate LEX Polynomial")
for fac in gb_lex[-1].factor():
    print(fac)
```

Algorithm 7 Code for Example 27.

```
q = 89
K = GF(q)
f = f = dickson_polynomial(7, K(1))
a = 1
b = 17
polys = c_boomerang_polynomials(f, a, b, c=-1)
I = ideal(polys)
gb = I.groebner_basis()
print("DRL Groebner Basis")
for poly in gb:
    print(poly)
print("")
gb_lex = ideal(gb).transformed_basis(algorithm="fglm")
print("Lexicographic Groebner Basis")
for poly in gb_lex:
    print(poly)
print("")
print("Factorization of Univariate LEX Polynomial")
for fac in gb_lex[-1].factor():
    print(fac)
```

Algorithm 8 Code for Example 28.

```
q = 191
K = GF(q)
P = PolynomialRing(K, "X")
X = P.gen()
f = X**3
a = 1
b = 125
polys = c_boomerang_polynomials(f, a, b, c=11)
I = ideal(polys)
gb = I.groebner_basis()
print("DRL Groebner Basis")
for poly in gb:
    print(poly)
print("")
gb_lex = ideal(gb).transformed_basis(algorithm="fglm")
print("Lexicographic Groebner Basis")
for poly in gb_lex:
    print(poly)
print("")
print("Factorization of Univariate LEX Polynomial")
for fac in gb_lex[-1].factor():
    print(fac)
```

References

[1] Eli Biham and Adi Shamir. "Differential Cryptanalysis of DES-like Cryptosystems". In: *Advances in Cryptology – CRYPTO'90*. Ed. by Alfred J. Menezes and Scott A. Vanstone. Vol. 537. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Aug. 1991, pp. 2–21. DOI: 10.1007/3-540-38424-3_1.

[2] Kaisa Nyberg. "Differentially Uniform Mappings for Cryptography". In: *Advances in Cryptology – EUROCRYPT'93*. Ed. by Tor Helleseth. Vol. 765. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, May 1994, pp. 55–64. DOI: 10.1007/3-540-48285-7_6.

[3] Pål Ellingsen, Patrick Felke, Constanza Riera, Pantelimon Stănică, and Anton Tkachenko. "C-Differentials, Multiplicative Uniformity, and (Almost) Perfect c-Nonlinearity". In: *IEEE Trans. Inf. Theory* 66.9 (2020), pp. 5781–5789. DOI: 10.1109/TIT.2020.2971988.

[4] David Wagner. "The Boomerang Attack". In: *Fast Software Encryption – FSE'99*. Ed. by Lars R. Knudsen. Vol. 1636. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Mar. 1999, pp. 156–170. DOI: 10.1007/3-540-48519-8_12.

[5] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. "Boomerang Connectivity Table: A New Cryptanalysis Tool". In: *Advances in Cryptology – EUROCRYPT 2018, Part II*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10821. Lecture Notes in Computer Science. Springer, Cham, Apr. 2018, pp. 683–714. DOI: 10.1007/978-3-319-78375-8_22.

[6] Pantelimon Stănică. "Investigations on c-boomerang uniformity and perfect nonlinearity". In: *Discrete Appl. Math* 304 (2021), pp. 297–314. ISSN: 0166-218X. DOI: 10.1016/j.dam.2021.08.002.

[7] Pantelimon Stănică. "Low c-differential and c-boomerang uniformity of the swapped inverse function". In: *Discrete Math.* 344.10 (2021), p. 112543. ISSN: 0012-365X. DOI: 10.1016/j.disc.2021.112543.

[8] Pantelimon Stănică. "Using double Weil sums in finding the c-boomerang connectivity table for monomial functions on finite fields". In: *Appl. Algebra Eng. Commun. Comput.* 34.4 (July 2023), pp. 581–602. ISSN: 1432-0622. DOI: 10.1007/s00200-021-00520-9.

[9] Sartaj Ul Hasan, Mohit Pal, and Pantelimon Stănică. "The binary Gold function and its c-boomerang connectivity table". In: *Cryptogr. Commun.* 14.6 (Nov. 2022), pp. 1257–1280. ISSN: 1936-2455. DOI: 10.1007/s12095-022-00573-8.

[10] Guanghui Li and Xiwang Cao. "The c-boomerang uniformity of two classes of permutation polynomials over finite fields". In: *Comput. Appl. Math.* 43.8 (Oct. 2024), p. 437. ISSN: 1807-0302. DOI: 10.1007/s40314-024-02956-4.

[11] Guanghui Li and Xiwang Cao. "The c-boomerang uniformity and c-boomerang spectrum of two classes of permutation polynomials over the finite field $\mathbb{F}_{2^n}$". In: *Discrete Math.* 348.9 (2025), p. 114543. ISSN: 0012-365X. DOI: 10.1016/j.disc.2025.114543.

[12] Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P. Smart. "MPC-Friendly Symmetric Key Primitives". In: *ACM CCS 2016: 23rd Conference on Computer and Communications Security*. Ed. by Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi. ACM Press, Oct. 2016, pp. 430–443. DOI: 10.1145/2976749.2978332.

[13] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. "MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity". In: *Advances in Cryptology – ASIACRYPT 2016, Part I*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10031. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Dec. 2016, pp. 191–219. DOI: 10.1007/978-3-662-53887-6_7.

[14] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. "Feistel Structures for MPC, and More". In: *ESORICS 2019: 24th European Symposium on Research in Computer Security, Part II*. Ed. by Kazue Sako, Steve Schneider, and Peter Y. A. Ryan. Vol. 11736. Lecture Notes in Computer Science. Springer, Cham, Sept. 2019, pp. 151–171. DOI: 10.1007/978-3-030-29962-0_8.

[15] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. "On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy". In: *Advances in Cryptology – EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. Lecture Notes in Computer Science. Springer, Cham, May 2020, pp. 674–704. DOI: 10.1007/978-3-030-45724-2_23.

[16] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. "Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields". In: *Advances in Cryptology – EUROCRYPT 2021, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. Lecture Notes in Computer Science. Springer, Cham, Oct. 2021, pp. 3–34. DOI: 10.1007/978-3-030-77886-6_1.

[17] Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch. "From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications". In: *Advances in Cryptology – EUROCRYPT 2023, Part IV*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. Lecture Notes in Computer Science. Springer, Cham, Apr. 2023, pp. 255–286. DOI: 10.1007/978-3-031-30634-1_9.

[18] Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. "Poseidon2: A Faster Version of the Poseidon Hash Function". In: *AFRICACRYPT 23: 14th International Conference on Cryptology in Africa*. Ed. by Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne. Vol. 14064. Lecture Notes in Computer Science. Springer, Cham, July 2023, pp. 177–203. DOI: 10.1007/978-3-031-37679-5_8.

[19] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. "New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode". In: *Advances in Cryptology – CRYPTO 2023, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, Cham, Aug. 2023, pp. 507–539. DOI: 10.1007/978-3-031-38548-3_17.

[20] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. "Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications". In: *Advances in Cryptology – CRYPTO 2023, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, Cham, Aug. 2023, pp. 573–606. DOI: 10.1007/978-3-031-38548-3_19.

[21] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. "Monolith: Circuit-Friendly Hash Functions with New Nonlinear Layers for Fast and Constant-Time Implementations". In: *IACR Transactions on Symmetric Cryptology* 2024.3 (2024), pp. 44–83. DOI: 10.46586/tosc.v2024.i3.44-83.

[22] Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan. "Can homomorphic encryption be practical?" In: *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*. CCSW '11. Chicago, Illinois, USA: Association for Computing Machinery, 2011, pp. 113–124. ISBN: 9781450310048. DOI: 10.1145/2046660.2046682.

[23] Tomer Ashur, Mohammad Mahzoun, and Dilara Toprakhisar. "Chaghri - A FHE-friendly Block Cipher". In: *ACM CCS 2022: 29th Conference on Computer and Communications Security*. Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. ACM Press, Nov. 2022, pp. 139–150. DOI: 10.1145/3548606.3559364.

[24] Jihoon Cho, Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Joohee Lee, Jooyoung Lee, Dukjae Moon, and Hyojin Yoon. "Transciphering Framework for Approximate Homomorphic Encryption". In: *Advances in Cryptology – ASIACRYPT 2021, Part III*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13092. Lecture Notes in Computer Science. Springer, Cham, Dec. 2021, pp. 640–669. DOI: 10.1007/978-3-030-92078-4_22.

[25] Yan-Ping Wang, Qiang Wang, and Wei-Guo Zhang. "Boomerang uniformity of normalized permutation polynomials of low degree". In: *Appl. Algebra Eng. Commun. Comput.* 31.3 (June 2020), pp. 307–322. ISSN: 1432-0622. DOI: 10.1007/s00200-020-00431-1.

[26] Matthias Johann Steiner. "A degree bound for the c-boomerang uniformity of permutation monomials". In: *Appl. Algebra Eng. Commun. Comput.* (Oct. 2024). ISSN: 1432-0622. DOI: 10.1007/s00200-024-00670-6.

[27] Shuhong Gao. "Absolute Irreducibility of Polynomials via Newton Polytopes". In: *J. Algebra* 237.2 (2001), pp. 501–520. ISSN: 0021-8693. DOI: 10.1006/jabr.2000.8586.

[28] Ulrich Görtz and Torsten Wedhorn. *Algebraic Geometry I: Schemes*. 2nd. Springer Studium Mathematik - Master. Springer Fachmedien Wiesbaden, 2020. ISBN: 978-3-658-30732-5. DOI: 10.1007/978-3-658-30733-2.

[29] Robin Hartshorne. *Geometry: Euclid and Beyond*. 1st ed. New York, NY: Springer New York, 2000. ISBN: 978-0-387-22676-7. DOI: 10.1007/978-0-387-22676-7.

[30] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 4th. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 978-3-319-16720-6. DOI: 10.1007/978-3-319-16721-3.

[31] Bruno Buchberger. "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal". PhD thesis. Universität Innsbruck, 1965.

[32] Gregor Kemper. *A Course in Commutative Algebra*. 1st ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. ISBN: 978-3-642-03545-6. DOI: 10.1007/978-3-642-03545-6.

[33] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. 1st. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000. ISBN: 978-3-540-67733-8. DOI: 10.1007/978-3-540-70628-1.

[34] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. 1st. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. ISBN: 978-3-540-28296-9. DOI: 10.1007/3-540-28296-3.

[35] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.7)*. 2025. URL: https://www.sagemath.org.

[36] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. "Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering". In: *Journal of Symbolic Computation* 16.4 (1993), pp. 329–344. ISSN: 0747-7171. DOI: 10.1006/jsco.1993.1051.

[37] Rudolf Lidl, Gary L. Mullen, and Gerhard Turnwald. *Dickson polynomials*. 1st. Pitman monographs and surveys in pure and applied mathematics. Longman Scientific & Technical, 1993. ISBN: 0 582 09119 5.

[38] Rudolf Lidl and Harald Niederreiter. *Finite fields*. 2nd. Encyclopedia of mathematics and its applications. Cambridge: Cambridge Univ. Press, 1997. ISBN: 0-521-39231-4.

[39] Arnab Roy and Matthias Johann Steiner. "Generalized Triangular Dynamical System: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields". In: *SAC 2024: 31st Annual International Workshop on Selected Areas in Cryptography, Part II*. Ed. by Maria Eichlseder and Sébastien Gambs. Vol. 15517. Lecture Notes in Computer Science. Springer, Cham, Aug. 2024, pp. 139–165. DOI: 10.1007/978-3-031-82841-6_6.