Noname manuscript No.
(will be inserted by the editor)

Algebraic properties of the maps χ_n

Jan Schoone · Joan Daemen

Received: date / Accepted: date

Abstract The Boolean map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ defined by $y_i = x_i + (x_{i+1} + 1)x_{i+2}$ (where $i \in \mathbb{Z}/n\mathbb{Z}$) is used in various permutations that are part of cryptographic schemes, e.g., Keccak-f (the SHA-3-permutation), ASCON (the winner of the NIST Lightweight competition), Xoodoo, Rasta and Subterranean (2.0). In this paper, we study various algebraic properties of this map. We consider χ_n (through vectorial isomorphism) as a univariate polynomial. We show that it is a power function if and only if $n = 1, 3$. We furthermore compute bounds on the sparsity and degree of these univariate polynomials, and the number of different univariate representations. Secondly, we compute the number of monomials of given degree in the inverse of χ_n (if it exists). This number coincides with binomial coefficients. Lastly, we consider χ_n as a polynomial map, to study whether the same rule ($y_i = x_i + (x_{i+1} + 1)x_{i+2}$) gives a bijection on field extensions of $\mathbb{F}_2$. We show that this is not the case for extensions whose degree is divisible by two or three. Based on these results, we conjecture that this rule does not give a bijection on any extension field of $\mathbb{F}_2$.

Keywords Boolean maps · chi · cryptography · polynomial maps · power functions · symmetric cryptography

Acknowledgements. The authors would like to thank Wieb Bosma and Marloes Venema, for proofreading (parts of) the text and giving helpful suggestions for improvement. This research is supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

Data availability statement

This manuscript has no associated data.

Jan Schoone
Digital Security, Radboud University, Nijmegen
E-mail: jan.schoone@ru.nl

Joan Daemen
Digital Security, Radboud University, Nijmegen

1 Introduction

In this paper, we consider the Boolean maps $\chi_n : \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ that are defined by $y_i = x_i + (x_{i+1} + 1)x_{i+2}$, with $i \in \mathbb{Z}/n\mathbb{Z}$. For $n = 5$, it is used in Keccak-f [2] (which is part of the NIST standard SHA-3 [22]) and ASCON [14] (the winner of the NIST lightweight competition [23]). For $n = 3$, it is used in Xoodoo [10]. Rasta [13] uses χ_n where n is the block-length (n is always odd). Lastly, Subterranean (2.0) ([7] and [11]) uses χ_{257}.

We know, from [8], that χ_n is invertible if and only if n is odd. Recently, from [20], we know a direct formula for χ_n^{-1}. The order of χ_n, and its cycle structure, are also known, see [28].

As χ_n is used in so many cryptographic applications, it is important to understand these maps very well. Each of the properties of χ_n could be exploited in an attack, or conversely be used to argue for security properties. For instance, in [8] and [9], the differential and correlation properties (related to differential [3] and linear [21] cryptanalysis) have been studied.

In this paper, we study some of the algebraic properties. E.g., the map χ_n can be represented by a univariate polynomial through an isomorphism $\mathbb{F}_2^n \cong \mathbb{F}_{2^n}$. This representation can be used to attack cryptographic ciphers (see, e.g., [6] and [15]). We study these univariate representations for χ_n to give insight in these representations.

The formula for χ_n^{-1} ([20]) gives rise to a simple question, that we answer in this paper. How many monomials of a certain degree occur in this formula?

Lastly, we might consider using the rule $y_i = x_i + (x_{i+1} + 1)x_{i+2}$ on field extensions (of $\mathbb{F}_2$) or finite fields of other characteristic.

Our contributions: We have studied the aforementioned algebraic properties and present the following results.

In Section 4, we discuss univariate polynomial expressions for the maps χ_n. In particular, we show that for $n \neq 1, 3$, they are not power functions. After that, we compute the number of different representations as a univariate polynomial with coefficients in the base field χ_n can take. This number is equal to $\underline{n} \cdot \varphi(n)$, where $\underline{n}$ is the number of normal elements in $\mathbb{F}_{2^n}$ and $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z}^*)$. Lastly, we give upper and lower bounds on the degree and sparsity of χ_n when given as a univariate polynomial.

Secondly, based on [20], we considered that there was no formula known for the number of monomials of a given degree in χ_n^{-1}. We compute those in Section 5. They behave according to binomial coefficients, i.e., the number of monomials of degree $m > 0$ in χ_n^{-1} is equal to $\binom{\frac{n+1}{2}}{m}$.

Thirdly, in Section 6, we view χ_n as a polynomial map (see [16]), and from that conclude that, if we take the same rule to define a $\chi_n^{(d)}$ over $\mathbb{F}_{2^d}$, it cannot be invertible for some d. We show that for even d and all d with $d \equiv 0 \pmod 3$, the map $\chi_n^{(d)}$ is not invertible, and conjecture that this holds for any $d > 1$.

We finalize this section by showing that the same rule will not give an invertible map in characteristic $p > 2$.

2 Notations and conventions

We write $\mathbb{F}_2$ for the finite field of two elements and $\mathbb{F}_m$ for a (finite) field of m elements. Additionally, we have the notation $\mathbb{F}_2^n$ for the standard n-dimensional $\mathbb{F}_2$-vector space, obtained as the Cartesian product of n copies of $\mathbb{F}_2$.

We write 0^n for the zero vector of n zeroes, and 1^n for the all-one vector of n ones.

The number of 1s in a sequence or vector x is called the *Hamming weight* and is denoted as $\mathrm{wt}(x)$.

We write $[\![v_1, \ldots, v_n]\!]$ for the (sub-)space spanned by the vectors $v_1, \ldots, v_n$.

We consider a basis to be an *ordered* set that is linearly independent and spanning. Therefore, we write them as tuples.

Thus $[\![v_1, \ldots, v_n]\!] = [\![v_2, v_1, v_3, \ldots, v_n]\!]$ give rise to isomorphic vector spaces, although we do consider the bases $(v_1, \ldots, v_n)$ and $(v_2, v_1, v_3, \ldots, v_n)$ distinct.

We write lg for the binary logarithm and R^* for the group of units of the ring R.

For a polynomial ring in one indeterminate X with coefficients in R, we write $R[X]$ and likewise for polynomial ring over n indeterminates $X_1, \ldots, X_n$, we write $R[X_1, \ldots, X_n]$.

3 χ_n and preliminary results

In this paper we study the maps χ_n:

Definition 1 **(χ_n)** Let $n \geq 1$. The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ is given by $y_i = x_i + (x_{i+1} + 1)x_{i+2} = x_i + x_{i+1}x_{i+2} + x_{i+2}$ where the indices are taken modulo n.

We see that each χ_n is a map of (algebraic) degree 2.

3.1 Shift maps and shift-invariant maps

A class of maps that is of interest with respect to χ is the class of shift maps.

Definition 2 **(Shift maps)** For any $n \geq 1$ and any $k \geq 0$ we can define two maps τ_n^k and τ_n^{-k} on $\mathbb{F}_2^n$, by iterating

$$\tau_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_{n-1}, x_0, x_1, \ldots, x_{n-2}).$$

We have $\tau_n^k = (\tau_n)^k$ and $\tau_n^{-k} = \tau_n^{(n-k)}$.

Definition 3 **(Shift-invariant maps)** A map $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *shift invariant* if we have $F \circ \tau_n^k = \tau_n^k \circ F$ for all $k \geq 0$.

By induction, we can relax the criterium for shift-invariance:

Lemma 1 *Similarly, a map $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is shift invariant if we have $F \circ \tau_n = \tau_n \circ F$.*

Using that $\tau_n^n = \mathrm{id}$, one can find the following generalization of Lemma 1.

Lemma 2 *Let* $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be a map, let* $k \geq 1$ *be such that* $\gcd(k,n) = 1$ *and* $\tau_n^k \circ F = F \circ \tau_n^k$. *Then* F *is shift invariant.*

Proof Since $\gcd(k,n) = 1$, there exists some integers a, l such that $ak = 1 + ln$. By induction to a, we know that $\tau_n^{ak} \circ F = F \circ \tau_n^{ak}$. Hence we have $\tau_n^{(1+ln)} \circ F = F \circ \tau_n^{(1+ln)}$. Since $\tau_n^n = \mathrm{id}$, we find that $\tau_n^{(1+ln)} = \tau_n$ and we are done by Lemma 1. $\square$

One immediately finds that all χ_n are shift invariant.

Lemma 3 *For each* n, $\chi_n\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *is shift invariant.*

As an example, we give a graph of χ_5 in Figure 1. Since χ_5 is shift invariant, for every input, the output can be deduced from this graph.

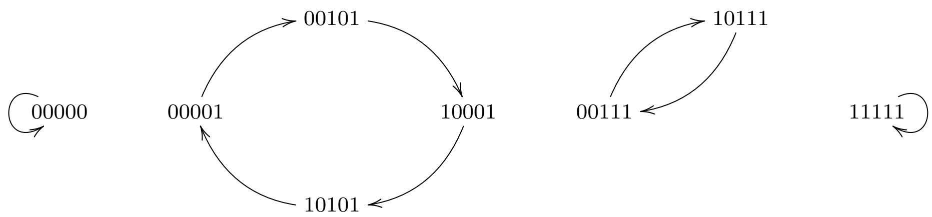

Fig. 1 Transformation of some binary vectors under χ_5.

3.2 Invertibility and order

From [8], we know that χ_n is invertible if and only if n is odd. Furthermore, we have a formula for the order of χ_n in this case.

Theorem 1 (Order of χ_n ([28])) *Let* $n > 0$ *be an odd integer. Then* $\mathrm{ord}(\chi_n) = 2^{\lceil \lg(\frac{n+1}{2}) \rceil}$.

In particular, we find that repeating χ_n for $2^{\lceil \lg(\frac{n+1}{2}) \rceil} - 1$ times, then this gives a way for computing the inverse. A direct formula for the inverse is determined in [20].

4 Univariate representations of χ_n

We can choose any isomorphism $\mathbb{F}_2^n \overset{\phi}{\cong} \mathbb{F}_{2^n}$ and consider $\chi_n^u\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ that is given by $\chi_n^u := \phi \circ \chi_n \circ \phi^{-1}$, as depicted in Figure 2.

This χ_n^u can be written as a univariate polynomial with coefficients in $\mathbb{F}_{2^n}$ by using Lagrange interpolation on all inputs. (See [29] and [19] (Thm 1.71).)

$$\begin{tikzcd} \mathbb{F}_2^n \arrow[r, "\chi_n"] \arrow[d, "\phi"'] & \mathbb{F}_2^n \arrow[d, "\phi"] \\ \mathbb{F}_{2^n} \arrow[r, "\chi_n^u"'] & \mathbb{F}_{2^n} \end{tikzcd}$$

Fig. 2 The schematics for the univariate χ_n.

With Lagrange interpolation on all pairs (t, u_t) one will find a polynomial $f(X) \in \mathbb{F}_{q^n}[X]$ that satisfies $u_t = f(t)$ and has degree $< q^n$. Note that by performing the interpolation on all inputs, one does not have to compute inverses, as:

$$f(t) = \sum_{i=0}^{2^n-1} f(x_i) \cdot \ell_i(t), \qquad \ell_i(t) = \prod_{\substack{i=0,\dots,2^n-1\\ i\neq j}} \frac{t - x_i}{x_j - x_i}$$

and we have

$$\prod_{\substack{i=0,\dots,2^n-1\\ i\neq j}} x_j - x_i = \prod_{\beta\in\mathbb{F}_{2^n}^*} \beta = \gamma^{\sum_{i=0}^{2^n-2} i} = \gamma^{\frac{1}{2}(2^n-2)(2^n-1)} = 1,$$

where γ is some generator of $\mathbb{F}_{2^n}^*$.

Definition 4 (Permutation polynomial) A polynomial $f(X) \in \mathbb{F}_{q^n}[X]$ is a *permutation polynomial* if its corresponding polynomial functions $t \mapsto f(t)$ is a permutation of $\mathbb{F}_{q^n}$.

Definition 5 (Equivalence of polynomials) Two polynomials $f(X), g(X) \in \mathbb{F}_{q^n}[X]$ are *functionally equivalent* if their corresponding polynomial functions $t \mapsto f(t)$ and $t \mapsto g(t)$ satisfy $f(t) = g(t)$ for all $t \in \mathbb{F}_{q^n}$.

It is straightforward that this is an equivalence relation. With a different criterion, we can see that there is always a representative of degree $< q^n$.

Proposition 1 (Equivalence Test ([19] 7.2)) *Two polynomials $f(X), g(X) \in \mathbb{F}_{q^n}[X]$ are functionally equivalent if and only if $f(X) \equiv g(X) \pmod{X^{q^n} - X}$*

We now give an example where we use Lagrange interpolation to find a polynomial representation of χ_3:

Example 1 Consider $\chi_3 \colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$ and the finite field $\mathbb{F}_{2^3} := \mathbb{F}_2(\alpha) = \mathbb{F}_2[X]/(X^3 + X + 1)$. Let $(1, \alpha, \alpha^2)$ be an ordered basis, then an isomorphism of vector spaces can be found as

$$\phi \colon \mathbb{F}_2^3 \to \mathbb{F}_{2^3},\ (x_0, x_1, x_2) \mapsto x_0 + \alpha \cdot x_1 + \alpha^2 \cdot x_2.$$

Then $\chi_3^u := \varphi \circ \chi_3 \circ \varphi^{-1}$ is given by: $0 \mapsto 0$, $1 \mapsto \alpha^3$, $\alpha \mapsto \alpha^4$, $\alpha^2 \mapsto \alpha^6$, $\alpha^3 \mapsto 1$, $\alpha^4 \mapsto \alpha$, $\alpha^5 \mapsto \alpha^5$ and $\alpha^6 \mapsto \alpha^2$. By using Lagrange interpolation, we find $\chi_3^u(X) \in \mathbb{F}_{2^3}[X]$ as

$$\chi_3^u(X) = \alpha^3 X^6 + \alpha^5 X^5 + \alpha^2 X^4 + \alpha^6 X^3 + \alpha X^2 + \alpha^2 X.$$

4.1 Power functions

A special kind of polynomials are those whose representative consists of a single monomial.

Definition 6 (Power functions) A *power function* is a polynomial function that can be represented by a single monomial in $\mathbb{F}_{q^n}[X]$. We write $(\cdot)^e\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ for a power function, here $e \geq 0$.

Since $\mathbb{F}_{q^n}^*$ is cyclic of order $q^n - 1$, we find that $t^{q^n-1} = 1$ for all $t \in \mathbb{F}_{q^n}^*$, hence $t^{q^n} = t$ for all $t \in \mathbb{F}_{q^n}$. Therefore, we only need to consider power functions with $0 \leq e < q^n - 1$. A power function is not necessarily a permutation polynomial.

Proposition 2 (Bijectivity ([19] 7.8)) *A power function* $(\cdot)^e\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ *is a permutation polynomial if and only if* $\gcd(e, q^n - 1) = 1$.

The set of all bijective power functions forms a group of order $\varphi(q^n - 1)$, which we denote as $\mathrm{Pow}(\mathbb{F}_{2^n})$. It is isomorphic to the automorphism group of $\mathbb{F}_{q^n}^*$, denoted as $\mathrm{Aut}(\mathbb{F}_{q^n}^*)$ (see [1] or [19] Ex 2.20).

Theorem 2 (Automorphisms are power functions) *Let n be a positive integer. Then* $\mathrm{Pow}(\mathbb{F}_{q^n}) = \mathrm{Aut}(\mathbb{F}_{q^n}^*)$.

It is also easy to express the order of a power function.

Proposition 3 (Order of power function) *The order of the power function* $(\cdot)^e$ *is given by the (multiplicative) order of e in* $\mathbb{Z}/(q^n - 1)\mathbb{Z}$.

Proof Note that $(\cdot)^e \circ (\cdot)^e = (\cdot)^{e^2}$, and similarly for k compositions: $(\cdot)^{e^k}$. □

Example 2 Consider $\mathrm{Pow}(\mathbb{F}_{2^9})$. It has $\varphi(2^9 - 1) = \varphi(511) = 6 \cdot 72 = 2^4 \cdot 3^2$ elements. There may exist power functions of order 8 in this group. By checking in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$, we find that for $e \in \{22, 83, 197, 209, 302, 314, 428, 489\}$ we have power functions of order 8.

4.2 Normal bases

Definition 7 (Normal basis [25]) Consider $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. Then $\beta \in \mathbb{F}_{q^n}$ is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if the set $\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{n-1}}\}$ is a linearly independent set. When considered as a tuple, this tuple is called a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Each element in a normal basis is a normal element. In [17] it is first proven that every finite extension field has a normal basis. In [25] the result is extended to giving the number of normal elements. In the following, when we will omit the *over* $\mathbb{F}_q$ and write β is a normal element of $\mathbb{F}_{q^n}$, or S is a normal basis of $\mathbb{F}_{q^n}$, when it is clear that they are considered *over* $\mathbb{F}_q$.

Example 3 Consider $\mathbb{F}_2 \subset \mathbb{F}_8$, with $\mathbb{F}_8 := \mathbb{F}_2(\alpha) = \mathbb{F}_2[X]/(X^3 + X + 1)$. Then α^3 is a normal element of $\mathbb{F}_8$:

$$\left[\!\!\left[\begin{array}{c} \alpha^3 \\ \alpha^6 \\ \alpha^5 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{c} \alpha+1 \\ \alpha^2+1 \\ \alpha^2+\alpha+1 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{c} \alpha+1 \\ \alpha^2+1 \\ \alpha^2 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{c} \alpha \\ 1 \\ \alpha^2 \end{array} \right]\!\!\right]$$

Therefore the tuple $(\alpha^3, \alpha^6, \alpha^5)$ is a normal basis. These normal elements are roots of $X^3 + X^2 + 1$.

With any choice of a normal element (and its corresponding normal basis) one obtains an isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$, as follows:

$$\varphi_\beta \colon \mathbb{F}_q^n \to \mathbb{F}_{q^n},\ (x_0, \ldots, x_{n-1}) \mapsto x_0\beta + \ldots + x_{n-1}\beta^{q^{n-1}}. \tag{1}$$

With the isomorphism φ_β, taking the qth power in $\mathbb{F}_{q^n}$ of an element corresponds to a shift of the coordinates in $\mathbb{F}_q^n$ in the following way:

Lemma 4 (([27] Lemma 5)) *Let β be a normal element of $\mathbb{F}_{q^n}$. Let φ_β be as in (1). Then $\varphi_\beta(\tau(x)) = \varphi_\beta(x)^q$.*

We now give an example of the representation of χ_3 as a univariate polynomial.

Example 4 Consider the map χ_3. Let α^3 be a normal element in $\mathbb{F}_{2^3}$ as in Example 3. We define $\chi_3^u := \varphi_{\alpha^3} \circ \chi_3 \circ \varphi_{\alpha^3}^{-1}$ with its inputs and outputs as given in columns 3 and 4 of Table 1. By using Lagrange interpolation we find that $\chi_3^u(t) = t^6$ for all t.

(a_0, a_1, a_2)	$\chi_3(a_0, a_1, a_2)$	$\varphi_{\alpha_3}(a_0, a_1, a_2)$	$\varphi_{\alpha_3}(\chi_3(a_0, a_1, a_2))$
$(0,0,0)$	$(0,0,0)$	0	0
$(0,0,1)$	$(1,0,1)$	α^5	α^2
$(0,1,0)$	$(0,1,1)$	α^6	α
$(0,1,1)$	$(0,1,0)$	α	α^6
$(1,0,0)$	$(1,1,0)$	α^3	α^4
$(1,0,1)$	$(0,0,1)$	α^2	α^5
$(1,1,0)$	$(1,0,0)$	α^4	α^3
$(1,1,1)$	$(1,1,1)$	1	1

Table 1 The maps χ_3 and χ_3^u.

We saw that $\chi_3^u(X) \in \mathbb{F}_2[X]$ in the previous example. We prove the more general theorem that any shift-invariant map has a univariate representation with coefficients in the base field.

Theorem 3 *Let $F \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a shift-invariant map. Let β be a normal element of $\mathbb{F}_{q^n}$ and φ_β as in (1). Consider the map $F^u \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined by $F^u := \varphi_\beta \circ F \circ \varphi_\beta^{-1}$. Then F^u is a polynomial function with $F^u(X) \in \mathbb{F}_q[X]$.*

Proof By Lemma 4 we find that $F^u(X^q) = F^u(X)^q$ since F is shift invariant. If we then write $F^u \in \mathbb{F}_{q^n}[X]$ as $\sum_{i=0}^m a_i X^i$ for some m, then we have

$$\sum_{i=0}^{m} a_i X^{iq} = F^u(X^q) = F^u(X)^q = \sum_{i=0}^{m} a_i^q X^{iq}.$$

Hence, $a_i^q = a_i$ for all $i = 0, \dots, m$ and thus $F^u(X) \in \mathbb{F}_q[X]$. □

Since χ_n is a shift-invariant map, we have the following immediate corollary:

Corollary 1 $\chi_n^u(X) \in \mathbb{F}_2[X]$.

4.3 The map χ_n^u is only a power function for $n = 1, 3$

The map χ_1 is the identity function, hence is equivalent to the power function with $e = 1$. We also found that for a suitable choice of normal basis, $\chi_3^u(X) = X^6$, a power function.

It is easy to see that for even n there is no power function equivalent to $\chi_n^u(X)$.

Lemma 5 *For any even n, there is no normal basis representation such that χ_n^u is a power function.*

Proof Suppose that there exists a normal basis representation such that χ_n^u is a power function. Since $\chi_n((01)^{n/2}) = 0^n$, there needs to exist some nonzero $\alpha \in \mathbb{F}_{2^n}$ with $\alpha^s = 0$ for some integer s, a contradiction. □

If $n > 3$ is a Mersenne-exponent, i.e., $2^n - 1$ is a prime number, then it is also easy to show that χ_n^u is not a power function.

Proposition 4 (Excluding Mersenne-exponents) *If $n > 3$ is such that $2^n - 1$ is a prime number, then there exists no normal basis representation of χ_n such that χ_n^u is a power function.*

Proof Since $2^n - 1$ is a prime number, then $\varphi(2^n - 1) = 2^n - 2$. Therefore, the only possibilities for the order of a power function are divisors of $2^n - 2$. By Theorem 1, the order of χ_n is divisible by 4 for all $n > 3$. The expression $2^n - 2$ has at most one factor 2, so there exists no power function that is equivalent to χ_n. □

For $n = 3$, we have $2^3 - 1 = 7$, a prime number. However, $\varphi(7) = 2 \cdot 3$ and χ_3 has order 2, so the proof of Proposition 4 does not hold for χ_3.

For the general case, we can prove that χ_n^u is not a power function by computing differential probabilities.

4.3.1 Differential probabilities

In this paragraph, we discuss differential probabilities, and with that show that χ_n is only a power function for $n = 1, 3$. Differential probabilities were studied in [3] as a way of breaking the cipher DES [24].

Definition 8 (Differential probability) Let $f\colon G \to H$ be a map between finite (additive) groups G and H. Let $g \in G$ and $h \in H$ be arbitrary. Then we define the *differential probability of f at (g,h)* as

$$\mathrm{DP}_f(g,h) = \#\{x \in G \mid f(x) - f(x-g) = h\}/|G|.$$

Example 5 (Differential distribution table of χ_3) Consider $\chi_3\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$, then we compute $\mathrm{DP}_{\chi_3}(g,h)$ for all $g,h \in \mathbb{F}_2^3$ and put them in a table, where the rows are indexed by g and columns are indexed by h. The dashes represent 0. Each entry in the table, DDT_{gh}, represents $\#\mathbb{F}_2^3 \cdot \mathrm{DP}_{\chi_3}(g,h)$ (see Table 2). Such a table we call a *differential distribution table*.

		output difference							
	χ_3	000	001	010	011	100	101	110	111
input difference	000	8	-	-	-	-	-	-	-
	001	-	2	-	2	-	2	-	2
	010	-	-	2	2	-	-	2	2
	011	-	2	2	-	-	2	2	-
	100	-	-	-	-	2	2	2	2
	101	-	2	-	2	2	-	2	-
	110	-	-	2	2	2	2	-	-
	111	-	2	2	-	2	-	-	2

Table 2 Differential distribution table (DDT) of χ_3.

In the next proposition we will show that the DDT is an invariant for (Boolean) functions.

Proposition 5 (Differential probabilities under linear isomorphisms) *Let $G \overset{\varphi}{\cong} H$ be isomorphic groups. Let $f\colon G \to G$ be a map and let $\widehat{f}\colon H \to H$ be the map induced through the isomorphism. Then $\mathrm{DP}_{\widehat{f}}(g,h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ for all $g,h \in H$.*

Proof We have

$$\begin{aligned}
\mathrm{DP}_{\widehat{f}}(g,h) &= \#\{x \in H \mid (\varphi \circ f \circ \varphi^{-1})(x) - (\varphi \circ f \circ \varphi^{-1})(x-g) = h\}/|H| \\
&= \#\{x \in H \mid (f \circ \varphi^{-1})(x) - f(\varphi^{-1}(x) - \varphi^{-1}(g)) = \varphi^{-1}(h)\}/|H| \\
&= \#\{y \in G \mid f(y) - f(y - \varphi^{-1}(g)) = \varphi^{-1}(h)\}/|G| \\
&= \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))
\end{aligned}$$

for all $g,h \in H$. □

One can similarly prove the following equalities for differential probabilities:

1. $\mathrm{DP}_{f+L}(g,h) = \mathrm{DP}_f(g, h - L(g))$;
2. $\mathrm{DP}_{f \circ L}(g,h) = \mathrm{DP}_f(L(g), h)$;
3. $\mathrm{DP}_{A \circ f}(g,h) = \mathrm{DP}_f(g, A^{-1}(h))$,

where the L and A are affine maps and A is, moreover, an invertible affine map. The differential properties of χ_n have been studied extensively (see [8], [9]). We say h is *compatible* with a g if $\mathrm{DP}_{\chi_n}(g, h) \neq 0$.

In the following, we will write a' and b' instead of g, h to coincide with the standard notation, where a' denotes an input difference, i.e., $a' = a + a^*$, and $b' = b + b^*$ an output difference. We will use the following result:

Proposition 6 (Differential probabilities for χ [8]) *Let $n > 1$ be an arbitrary odd integer and $a' \in \mathbb{F}_2^n$. Then for any $b' \in \mathbb{F}_2^n$ compatible with a', we have $\mathrm{DP}_{\chi_n}(a', b') = 2^{-w(a')}$, where*

$$w(a') = \begin{cases} n-1 & \text{if } a' = 1^n; \\ \mathrm{wt}(a') + r_{a'} & \text{else.} \end{cases}$$

where $r_{a'}$ is the number of 001-subsequences in a'.

Since we have been unable to find a complete proof of this result in the literature, we include our own proof in Appendix 7.1.

For power functions, the differential probabilities have also been studied, in e.g., [4]:

Proposition 7 (Differential probabilities for power functions [4]) *Let $0 \leq e \leq 2^n - 1$ and let $f = (\cdot)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a power function. Then $\mathrm{DP}_f(a', b') = \mathrm{DP}_f(ya', y^e b')$ for all $y \in \mathbb{F}_{2^n}^*$.*

In particular, if we compute $\mathrm{DP}_f(1, b')$ for all b', we can use the above proposition to deduce the remainder of the differential distribution table. As a direct corollary, we see that the number of occurrences of 0 is the same in every row (except the first), and the same holds for the number of occurrences of $2, 4, \ldots$.

Example 6 (Differential distribution table of $t \mapsto t^6$) Let $\mathbb{F}_8$ be determined by $X^3 + X + 1$ and consider $(\cdot)^6 \colon \mathbb{F}_8 \to \mathbb{F}_8$. Then in Table 3, one sees the differential distribution table for $(\cdot)^6$.

		output difference							
	$(\cdot)^6$	0	1	x	x^2	x^3	x^4	x^5	x^6
input difference	0	8	-	-	-	-	-	-	-
	1	-	2	-	-	2	-	2	2
	x	-	-	-	2	-	2	2	2
	x^2	-	-	2	-	2	2	2	-
	x^3	-	2	-	2	2	2	-	-
	x^4	-	-	2	2	2	-	-	2
	x^5	-	2	2	2	-	-	2	-
	x^6	-	2	2	-	-	2	-	2

Table 3 The DDT of $t \mapsto t^6$.

We can now use what we know about differential properties of χ_n and power functions to prove:

Theorem 4 (χ_n is not a power function for $n \neq 1, 3$) *Let $n \neq 1, 3$ be a positive integer. Then there exists no way to write χ_n^u as a power function.*

Proof Let $n \neq 1, 3$ be an arbitrary odd positive integer. (The even case has been proven in Lemma 5.) Consider any isomorphism from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$ under which χ_n would become χ_n^u. By Proposition 5, we find that their differential distribution should be similar. Set $a' = 110^{n-2}$ and $a'' = 10^{n-1}$. Then we find that $\mathrm{DP}_{\chi_n}(a', b') = \frac{1}{8}$ and $\mathrm{DP}_{\chi_n}(a'', b') = \frac{1}{4}$ for all b' that are compatible with a', a'' respectively, by Proposition 6. Whereas, by Proposition 7, we have that each row of the DDT should have the same number of occurrences of $0, 2, 4, \ldots$. Therefore, χ_n^u cannot be a power function. $\square$

Example 7 (Two rows in DDT_{χ_5}*)* When computing the rows in DDT_{χ_5} coinciding with input differences $a'11000$ and $a'' = 10000$ as in the proof of the preceding theorem, the row coinciding with a' has sixteen 2s and the row coinciding with a'' has eight 4s.

Definition 9 (Extended affine equivalence) Let F and G be two Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We say that F and G are *extended affine equivalent* if there exist:

- an affine permutation A of $\mathbb{F}_2^n$;
- an affine permutation B of $\mathbb{F}_2^m$; and
- an affine map $C\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$,

such that $G = (B \circ F \circ A) + C$.

We obtain, by using the properties for differential probability listed after Proposition 5, as a direct corollary to Theorem 4:

Corollary 2 *Let $n \neq 1, 3$ be a positive integer. Let F be any extended affine equivalent of χ_n. Then F^u is not a power function.*

4.4 Number of different univariate polynomial representations of χ_n.

A priori, since we make several choices, there could be many different univariate representations of χ_n for each n. In this section, we go over the choices we make and discuss how they affect the outcome of the univariate representation. In order, we discuss the choice of representation of the field, i.e., the irreducible polynomial of degree n that defines $\mathbb{F}_{2^n}$. After that, we treat how different normal elements may give rise to different univariate polynomial representations. Each normal element β has a canonical ordered basis, yielding an isomorphism φ_β as in Equation 1. But there might be basis transformations, that shuffle the basis elements. This will provide a different isomorphism from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$, and in some cases it will give a univariate polynomial in the base field.

Choosing an irreducible polynomial to create the field extension It is a well-known result that for any prime power there exists (up to isomorphism) a unique field with that many elements. Does this “up to isomorphism” interfere with the univariate expression of a map? The isomorphism φ_β is defined by the normal element. This normal element is defined by being a root of a polynomial. In fact, if the degree of this polynomial is d, then there are d roots, all of which are normal elements.

Proposition 8 *Let $\mathbb{F}_f := \mathbb{F}_2[X]/(f(X))$ and $\mathbb{F}_g := \mathbb{F}_2[X]/(g(X))$ be isomorphic fields. Let α be a normal element in $\mathbb{F}_f$ that is a root of the polynomial $h(X) \in \mathbb{F}_2[X]$. Then there exists some $\beta \in \mathbb{F}_g$ that is a normal element as a root of $h(X)$. Furthermore, $\beta, \beta^2, \ldots, \beta^{2^{\deg f - 1}}$ are all roots of $h(X)$.*

Proof Let $\psi\colon \mathbb{F}_f \to \mathbb{F}_g$ be an isomorphism. Then since $h(\alpha) = 0$, we must have $\psi(h(\alpha)) = \psi(0) = 0$. Since ψ is a field-homomorphism, we find that $\psi(h(\alpha)) = h(\psi(\alpha))$ as a polynomial equation consists solely of additions and multiplications. Therefore $\beta = \psi(\alpha)$ is also a root of $h(X)$.

For the second statement we note that $(a+b)^{2^i} = a^{2^i} + b^{2^i}$ for $i \geq 0$ since we work in a field of characteristic 2. Therefore $h(\alpha^{2^i}) = h(\alpha)^{2^i} = 0$ for all $i \in \{0, \ldots, \deg f - 1\}$. □

Since $\mathbb{F}_{2^n}^*$ is cyclic for any n, we find that any normal element generates the entire group. As the isomorphism ψ maps normal elements to linear combinations between powers of the same normal element, we therefore find that the "up to isomorphism" indeed does not influence the univariate expression of a map.

Choice of the normal element We have a choice on the normal elements that we make in defining a univariate expression. This choice of normal element influences the resulting univariate expression, in particular, if β, γ are two distinct normal elements such that γ is not in any normal basis containing β, then we get different univariate polynomials.

From [19] (Thm 3.73), or [25], we obtain the following formula for the number of distinct normal elements:

Theorem 5 (Number of normal elements) *Let q be a prime power and $m \geq 1$ an integer. There exist precisely $\Phi_q(X^m - 1)/m$ normal elements in $\mathbb{F}_{q^m}$ (w.r.t. $\mathbb{F}_q$).*

Here, $\Phi_q(f)$ denotes the number of polynomials in $\mathbb{F}_q[X]$ that are coprime to f and have a smaller degree than $\deg(f)$.

We will denote the number of normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$) by $\underline{n}$. Thus, $\underline{n} = \Phi_2(X^n - 1)/n$.

(Re-)Ordering the normal basis Given a normal basis $(\beta, \beta^q, \ldots, \beta^{q^{n-1}})$ of $\mathbb{F}_{q^n}$, there are several ways to re-order the elements in this basis. In particular, for every permutation $\sigma \in S_n := \mathrm{Sym}(\{0, \ldots, n-1\})$ we have a re-ordered basis by $(\beta^{\sigma(0)}, \beta^{\sigma(1)}, \ldots, \beta^{q^{\sigma(n-1)}})$.

Then we can define the isomorphism

$$\varphi_\beta^\sigma\colon (x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i \beta^{q^{\sigma(i)}} \tag{2}$$

as the isomorphism corresponding to the one in (1) when the basis is re-ordered. (Note that the isomorphism given in (1) is the one where σ is the identity permutation.) A priori therefore, there are $n!$ different univariate representations when the normal basis is fixed.

We indicate that a left-shift over the basis elements corresponds with the permutation $\sigma = \big(0\ 1\ 2 \cdots\ n-1\big)$. We can therefore write $\varphi_\beta^{\sigma\circ\tau^k} := \varphi_\beta^\sigma \circ \tau^k$. In the case that a map F is shift invariant, we can immediately reduce the number of representations to $(n-1)!$:

Lemma 6 *Let β be a normal element in $\mathbb{F}_{q^n}$ and $F\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ a shift-invariant map. Let $\varphi := \varphi_\beta$ be as in (1) and $k \in \{1, \ldots, n-1\}$ be arbitrary. Consider the isomorphism $\psi := \varphi^{\tau^k}$. Write F_ψ^u for the corresponding univariate representation of F. Then $F_\psi^u = F_\varphi^u$.*

Proof Using the Lagrange interpolation formula, we get

$$\begin{aligned} F_\psi^u(t) &= \sum_{v\in\mathbb{F}_q^n} (\psi \circ F)(v) \cdot \ell_{\psi(v)}(t) \\ &= \sum_{v\in\mathbb{F}_q^n} (\varphi \circ \tau^k \circ F)(v) \cdot \ell_{(\varphi\circ\tau^k)(v)}(t) \\ &= \sum_{v\in\mathbb{F}_q^n} (\varphi \circ F \circ \tau^k)(v) \cdot \ell_{(\varphi\circ\tau^k)(v)}(t) \\ &= \sum_{v'\in\mathbb{F}_q^n} (\varphi \circ F)(v') \cdot \ell_{\varphi(v')}(t) \\ &= F_\varphi^u(t) \end{aligned}$$

as required. □

Remark 1 Since $\varphi_\beta \circ \tau^k \colon (x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_{i+k \bmod n}\beta^{q^{i+k \bmod n}}$, we find that the univariate expression is invariant under a shift of the coefficients, as expected. Thus we can assume, without loss of generality, that $\sigma(0) = 0$. The same result holds when we have a re-ordered normal basis, thus for φ_β^σ.

We will now investigate which re-orderings yield univariate expressions with coefficients in the base field. In the proof of Theorem 3 we use Lemma 4. Therefore it is prudent to look for ismorphisms under which taking a qth power corresponds to some shift coprime in length to the dimension of the domain of$F$. (See Lemma 2.)

Let $\gcd(k, n) = 1$. We want to solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^q \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We first illustrate this with an example.

Example 8 Let q be an arbitrary prime power, $n = 5$ and $k = 3$. We have the following commuting diagram by hypothesis:

$$\begin{tikzcd}
(x_0,x_1,x_2,x_3,x_4) \arrow[r, mapsto, "\varphi_\beta^\sigma"] \arrow[dd, mapsto, "\tau^3"'] & x_0\beta + x_1\beta^{q^{\sigma(1)}} + x_2\beta^{q^{\sigma(2)}} + x_3\beta^{q^{\sigma(3)}} + x_4\beta^{q^{\sigma(4)}} \arrow[d, mapsto, "(\cdot)^q"] \\
& x_0\beta^q + x_1\beta^{q^{\sigma(1)+1}} + x_2\beta^{q^{\sigma(2)+1}} + x_3\beta^{q^{\sigma(3)+1}} + x_4\beta^{q^{\sigma(4)+1}} \arrow[d, equal] \\
(x_3,x_4,x_0,x_1,x_2) \arrow[r, mapsto, "\varphi_\beta^\sigma"'] & x_3\beta + x_4\beta^{q^{\sigma(1)}} + x_0\beta^{q^{\sigma(2)}} + x_1\beta^{q^{\sigma(3)}} + x_2\beta^{q^{\sigma(4)}}
\end{tikzcd}$$

From this diagram we find the following equations

$$0 = \sigma(3) + 1, \quad \sigma(1) = \sigma(4) + 1, \quad \sigma(2) = 1, \quad \sigma(3) = \sigma(1) + 1, \quad \sigma(4) = \sigma(2) + 1.$$

Therefore, we easily obtain $\sigma = (1\ 3\ 4\ 2)$.

Lemma 7 *Consider a finite field extenstion $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ with a normal element β. Let $0 \leq k \leq n-1$ be such that $\gcd(k,n) = 1$. Then there exists a unique σ such that $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^q \circ \varphi_\beta^\sigma$.*

Proof Write $\mathbf{x}$ for the vector $(x_0, \dots, x_{n-1})$. We have $\varphi_\beta^\sigma(\mathbf{x}) = \sum_{i=0}^{n-1} x_i \beta^{q^{\sigma(i)}}$ and

$$\varphi_\beta^\sigma(\tau^k(\mathbf{x})) = \sum_{i=0}^{n-1} x_{i-k \bmod n} \beta^{q^{\sigma(i)}} = \sum_{j=0}^{n-1} x_j \beta^{q^{\sigma(j+k \bmod n)}}.$$

Then from the hypothesis $\gcd(k,n)$, we find that $(\varphi_\beta^\sigma(\mathbf{x}))^q = \varphi_\beta^\sigma(\tau^k(\mathbf{x}))$ we find that, for indices $j, j+k$ modulo n, $\sigma(j+k) = \sigma(j) + 1$. Since by Lemma 6 we can take $\sigma(0) = 0$, we can deduce $\sigma(k) = 1$ and $\sigma(n-k) = n-1$. Since k is invertible in $\mathbb{Z}/n\mathbb{Z}$, the entire structure of σ is then uniquely determined. □

We conclude that given an irreducible polynomial and a normal element, there are $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z}^*)$ different univariate polynomial representations with coefficients in the prime field.

Taking into account the number of different normal elements, we obtain:

Theorem 6 *Let $n > 0$ be an arbitrary odd integer. Then there are $\underline{n} \cdot \varphi(n)$ different univariate polynomial representations of χ_n with coefficients in $\mathbb{F}_2$.*

Some numbers of different univariate polynomial representations of χ_n:

n	3	5	7	9	11	13	15	17
$\underline{n}$	1	3	7	21	93	315	675	3825
$\varphi(n)$	2	4	6	6	10	12	8	16
$\underline{n} \cdot \varphi(n)$	2	12	42	126	930	3780	5400	61200

Table 4 The number of different univariate polynomial representations of a given shift-invariant map.

4.5 Bounds on degrees and sparsity

Irrespective of any choices, we can easily show certain facts on upper and lower bounds on the degree of the univariate expression and the sparsity of the univariate expressions.

We have various notions of degree. For instance, if we write χ_3 as in Definition 1, we see that χ_3 has degree 2. However, if we consider χ_3 as a univariate polynomial as in Example 1, we see that $\chi_3(X)$ has degree 6. In order to make some sense of this, we explain the several different notions of degree.

Definition 10 (Algebraic normal form (ANF) and algebraic degree) Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a (Boolean) map in its *algebraic normal form*, that is, each F_i is given as a multivariate polynomial in n variables, that is a sum of monomials. Then, the degree of a coordinate function F_i is the maximum of the degrees of its monomials. A monomial $X_1^{e_1} \cdots X_r^{e_r}$ has degree $e_1 + \ldots + e_r$. Then the *algebraic degree* of F, denoted by $\deg_a(F)$, is the maximum of the degrees of each of the F_i.

When $m = 1$, the algebraic degree corresponds with the usual degree.

Definition 11 (Two-degree) Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a map given by a univariate polynomial. Write $F(X) = \sum_{j=0}^{2^n-1} c_j X^j$. Then the 2-*degree* of F is given by

$$\deg_2(F) = \max\{\mathrm{w}_2(j) \mid 0 \leq j \leq 2^n - 1, c_j \neq 0\},$$

where $\mathrm{w}_2(j)$ is the Hamming-weight of j in its binary expansion.

Example 9 We continue from Example 1. We see that the exponents of X where there is a non-zero coefficient are $6, 5, 4, 3, 1$. The list of their respective $\mathrm{w}_2(j)$ is $2, 2, 1, 2, 1$. Hence we see that the 2-degree of χ_3^u is 2.

The phenomenon in the previous example is not a one-time occurrence. It holds in general, as stated in the following proposition.

Proposition 9 (Algebraic degree and 2-degree) *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a given (Boolean) map in its ANF. Let $F(X) \in \mathbb{F}_{2^n}[X]$ be the corresponding univariate polynomial. Then $\deg_a(F) = \deg_2(F(X))$.*

We refer to [5] for the proof of this result.

The bounds that we are going to prove in this section are on the regular degree of the univariate polynomial. Since we know that χ_n has algebraic degree 2, we know that its 2-degree should be 2 as well. This means that the only powers of t in $\chi_n^u(t)$ have Hamming-weight at most 2. The largest possible such number is then $2^{n-1} + 1$, since the powers of t are already bounded by $2^n - 1$. Likewise the lowest possible degree for $\chi_n^u(t)$ is 3.

We list some of these bounds in the following table:

n	3	5	7	9	11	13	15	17
$\max \deg_a(\chi_n^u)$	6	24	96	384	1536	6144	24576	98304
$2^n - 1$	7	31	127	511	2047	8191	32767	131071

Table 5 Upper bounds on the degree of univariate expressions.

By the same line of reasoning, we have an immediate formula for the sparsity of $\chi_n^u(t)$, by the 2-degree. We obtain that the number of monomials in $\chi_n^u(t)$ is at most $\binom{n}{1} + \binom{n}{2}$. Each possible exponent can be written in a binary sequence of length n. We allow only those where there is one 1, or two 1s.

We list some of these bounds in the following table:

In Appendix 7.2, we give a table of the minimum and maximum sparsity of (actually occurring) univariate expressions of χ_n, as well as the minimum and maximum occurring degrees.

We furthermore list the univariate polynomial representations of χ_n for $n \leq 7$.

n	3	5	7	9	11	13	15	17
max. mon. in χ_n^u	6	15	28	45	66	91	120	153
2^n	8	32	128	512	2048	8192	32768	131072

Table 6 Sparsity of univariate expressions.

5 Monomial count of χ_n^{-1}

We find in [20] that the inverse of χ_n^{-1} has a nice expression:

Theorem 7 **(χ_n^{-1} ([20]))** *For odd $n > 0$, the formula for χ_n^{-1} is given by:*

$$x_i = y_i + \sum_{j=1}^{(n-1)/2} y_{i-2j+1} \prod_{k=j}^{(n-1)/2} \overline{y_{i-2k}}.$$

The degree of χ_n^{-1} is thus $(n+1)/2$.

For some use-cases, having this formula and its degree is enough as exhibited in [20]. However, for several cases, like algebraic attacks, one might use the monomial count, e.g., [12]. In any case, it is an interesting number to compute, and it turns out to follow a beautiful formula. We investigate in this section the total monomial count, and the number of monomials of a given degree in any one of the coordinates of χ_n^{-1}.

Definition 12 **(Monomials of certain degree)** Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function expressed as a multivariate polynomial. Any term in this multivariate polynomial of the form $x_{i_1}^{e_{i_1}} \cdots x_{i_k}^{e_{i_k}}$ for some k is called a *monomial*. The (algebraic) degree of this monomial is $e = e_{i_1} + \ldots + e_{i_k}$ (as in Definition 10). We write $\mathcal{M}_e(f_i)$ for the set of monomials of degree e in the component f_i.

Example 10 Consider χ_n as in Definition 1. Then each component has the form $y_i = x_i + (x_{i+1} + 1)x_{i+2} = x_i + x_{i+2} + x_{i+1}x_{i+2}$. Then $\mathcal{M}_1(\chi_{n,i}) = \{x_i, x_{i+2}\}$ and $\mathcal{M}_2(\chi_{n,i}) = \{x_{i+1}x_{i+2}\}$ for each $n > 0$ and each $0 \le i < n$.

From Theorem 7, we can determine the following:

Proposition 10 **(Monomial count of χ_n^{-1})** *For each odd $n > 0$ and each $0 < m \le \frac{n+1}{2}$, we have*

$$\#\mathcal{M}_m(\chi_{n,i}^{-1}) = \binom{\frac{n+1}{2}}{m}.$$

For the proof, we use the following combinatorial lemma, which is a repeated application of Pascal's Rule [26], and is very similar to the Hockey Stick Identity ([18]):

Lemma 8 *Let n be a positive integer. Then for all $0 \le k < n$ we have*

$$\sum_{i=0}^{k} \binom{n-i}{k-i} = \binom{n+1}{k}. \tag{3}$$

Remark 2 Using the rule $\binom{n}{k} = \binom{n}{n-k}$ we also get the following formula:

$$\sum_{i=0}^{n-j} \binom{n-i}{j} = \binom{n+1}{j+1}.$$

Proof (of Proposition 10) Let $h = \frac{n-1}{2}$. By working through the summation symbol, we find the numbers as in Table 7.

For instance, to count the number of monomials of degree $h-3$ that occur in the summation when $j = 2$, we note that we have $h-1$ terms in the product, where at each time we have either the 1-term, or the degree-1-term. To get a degree of $h-3$, we need to have precisely two times the 1-term, or - in other words - $h-3$ times the degree-1-term. The number of possibilities is then given by $\binom{h-1}{h-3}$.

Or, to count the number of monomials of degree 3 that occur when $j = 4$, we have in the product exactly $h-3$ terms. Of those, precisely two times we must choose, the degree-1-term, or, precisely $h-5$ times the constant term.

Finally, $\mathrm{m}_i = \#\mathcal{M}(\chi_{n,i}^{-1})$ is the sum of all numbers in the column of m_i.

By Lemma 8, or, equivalently, the formula in the remark after this lemma, we then find the desired equalities, except for m_1, where we need to add the single degree-1-monomial y_i. □

j	m_{h+1}	m_h	m_{h-1}	m_{h-2}	m_{h-3}	$\cdots$	m_4	m_3	m_2	m_1
$j=1$	1	$\binom{h}{h-1}$	$\binom{h}{h-2}$	$\binom{h}{h-3}$	$\binom{h}{h-4}$	$\cdots$	$\binom{h}{3}$	$\binom{h}{2}$	$\binom{h}{1}$	1
$j=2$	-	1	$\binom{h-1}{h-1}$	$\binom{h-1}{h-2}$	$\binom{h-1}{h-3}$	$\cdots$	$\binom{h-1}{3}$	$\binom{h-1}{2}$	$\binom{h-1}{1}$	1
$j=3$	-	-	1	$\binom{h-2}{h-1}$	$\binom{h-2}{h-2}$	$\cdots$	$\binom{h-2}{3}$	$\binom{h-2}{2}$	$\binom{h-2}{1}$	1
$j=4$	-	-	-	1	$\binom{h-3}{h-1}$	$\cdots$	$\binom{h-3}{3}$	$\binom{h-3}{2}$	$\binom{h-3}{1}$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j=h$	-	-	-	-	-	$\cdots$	-	-	1	1

Table 7 The numbers m_i of monomials of degree i, for each summand j. Here $h = \frac{n-1}{2}$.

Since we have determined the number of monomials of each degree $1 \le m < \frac{n+1}{2}$, we can immediately deduce the total number of monomials in any coordinate of χ_n^{-1}.

Corollary 3 (Monomials in χ_n^{-1}) *Let $n > 0$ be odd, then the total number of monomials in any coordinate of χ_n^{-1} is equal to $2^{\frac{n+1}{2}} - 1$.*

6 χ as a polynomial map

In the field of affine algebraic geometry, the morphisms between varieties are the polynomial maps.

Definition 13 (Polynomial map) Let k be an arbitrary ring, and $k[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates. A *polynomial map* is a map $F = (F_1, \ldots, F_n)\colon k^n \to k^n$ of the form

$$(x_1, \ldots, x_n) \mapsto (F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n)),$$

where each $F_i \in k[X_1, \ldots, X_n]$.

We can observe the related polynomial map of χ_n in n variables. This is given by

$$\Xi_n(X_1,\ldots,X_n) = (X_1 + (X_2+1)X_3, X_2 + (X_3+1)X_4, \ldots, X_n + (X_1+1)X_2).$$

A polynomial map is invertible if there exists a polynomial map $G\colon k^n \to k^n$ such that

$$X_i = G_i(F_1,\ldots,F_n),$$

for all $1 \le i \le n$. By checking the determinant of the Jacobian, we can check whether Ξ_n is invertible.

For χ_n we have the following form for the Jacobian:

$$\mathrm{Jac}_{\Xi_n} = \begin{pmatrix} 1 & X_3 & X_2+1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & X_4 & X_3+1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & X_5 & X_4+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ X_n+1 & 0 & 0 & 0 & 0 & \cdots & X_1 \\ X_2 & X_1+1 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

If $|\,\mathrm{Jac}_{\Xi_n}\,| = 1$, then Ξ_n is invertible.

Proposition 11 (χ_n is not invertible as a polynomial map) *The polynomial map Ξ_n is not invertible on $\mathbb{F}_2$.*

Proof The determinant $|\,\mathrm{Jac}_{\Xi_n}\,|$ contains a term $(-1)^{n+1}X_2 \cdot |M_{n,1}|$, where $M_{n,1}$ is the minor where the nth row and first column are deleted from the Jacobian. This factor does not cancel out, as can be seen from the shape of the matrix. $\square$

Example 11 ($|\,\mathrm{Jac}_{\Xi_3}\,|$) We compute the determinant of $\mathrm{Jac}(\Xi_3)$:

$$\begin{aligned} |\,\mathrm{Jac}(\Xi_3)| &= 1 \cdot \begin{vmatrix} 1 & X_1 \\ X_1+1 & 1 \end{vmatrix} + (X_3+1)\begin{vmatrix} X_3 & X_2+1 \\ X_1+1 & 1 \end{vmatrix} + X_2 \begin{vmatrix} X_3 & X_2+1 \\ 1 & X_1 \end{vmatrix} \\ &= 1 + X_1(X_1+1) + (X_3+1)X_3 + (X_3+1)(X_2+1)(X_1+1) \\ &\quad + X_2X_3X_1 + X_2(X_2+1) \\ &= X_1^2 + X_2^2 + X_3^2 + X_1X_2 + X_1X_3 + X_2X_3. \end{aligned}$$

Remark 3 The (in)famous Jacobian Conjecture states that a polynomial map is invertible if and only if the determinant of its Jacobian is invertible. Here, we used the easy-to-prove necessary condition.

Definition 14 (χ_n on field extensions) Let $\mathbb{F}_{2^k}$ be a field extension of $\mathbb{F}_2$. We define $\chi_n^{(k)}$ as the polynomial function indicated by the polynomial map Ξ_n on the field $\mathbb{F}_{2^k}$.

Note that with this definition $\chi_n^{(1)} = \chi_n$.

Since Ξ_n is not invertible, while χ_n is invertible on $\mathbb{F}_2^n$, for odd n, it means that for some field extension of $\mathbb{F}$, the polynomial function $\chi_n^{(k)}$ is not invertible. This is due to the following result:

Proposition 12 ([16] Thm 4.2.1) *Let K be an algebraically closed field. Let $F\colon K^n \to K^n$ be a polynomial function that is invertible. Then F is invertible as a polynomial map.*

Example 12 (χ_3 on $\mathbb{F}_4$) Consider the map

$$\chi_3^{(2)}\colon \mathbb{F}_4^3 \to \mathbb{F}_4^3,\ (x_0, x_1, x_2) \mapsto (x_0 + (x_1 + 1)x_2, x_1 + (x_2 + 1)x_0, x_2 + (x_0 + 1)x_1).$$

Note that in $\mathbb{F}_4$ we have an element α with $\alpha^2 + \alpha + 1 = 0$. Take the elements $(\alpha, 1, \alpha)$, $(\alpha, \alpha, 0)$, $(\alpha^2, \alpha, \alpha)$ and $(\alpha^2, 0, 1)$. They all are mapped to $(\alpha, 0, 1)$ under $\chi_3^{(2)}$:

$$\begin{aligned}
\chi_3^{(2)}(\alpha, 1, \alpha) &= (\alpha + 0 \cdot \alpha, 1 + (\alpha + 1)\alpha, \alpha + (\alpha + 1) \cdot 1) \\
&= (\alpha, \alpha^2 + \alpha + 1, \alpha + \alpha + 1) = (\alpha, 0, 1) \\
\chi_3^{(2)}(\alpha, \alpha, 0) &= (\alpha + (\alpha + 1) \cdot 0, \alpha + \alpha, 0 + (\alpha + 1)\alpha) \\
&= (\alpha, 0, \alpha^2 + \alpha) = (\alpha, 0, 1) \\
\chi_3^{(2)}(\alpha^2, \alpha, \alpha) &= (\alpha^2 + (\alpha + 1)\alpha, \alpha + (\alpha + 1)\alpha^2, \alpha + (\alpha^2 + 1)\alpha) \\
&= (\alpha^2 + \alpha^2 + \alpha, \alpha + \alpha^3 + \alpha^2, \alpha + \alpha^3 + \alpha) = (\alpha, 0, 1) \\
\chi_3^{(2)}(\alpha^2, 0, 1) &= (\alpha^2 + 1, 0 + 0 \cdot \alpha^2, 1 + (\alpha^2 + 1) \cdot 0) \\
&= (\alpha, 0, 1).
\end{aligned}$$

It is therefore clear that $\chi_3^{(2)}$ is not invertible.

The previous example generalizes for any odd $n > 1$. Since χ_n is not invertible for even n, we immediately have $\chi_n^{(k)}$ is not invertible either, for any $k > 1$.

Conjecture 1 (χ_n is not invertible on any field extensions of $\mathbb{F}_2$) Let n, k be integers, both greater than 1 and n odd. Then $\chi_n^{(k)}\colon \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ is not invertible.

We conjecture the above, because we have found proofs for all even k and all k that are multiples of 3, as below. Note that we have $\mathbb{F}_{2^m} \subset \mathbb{F}_{2^l}$ if and only if $m \mid l$, hence we only have to check $k = 2$ and $k = 3$, as those examples work immediately in any extension of $\mathbb{F}_{2^2}$ or $\mathbb{F}_{2^3}$.

Proof (for $k = 2$:) Let $n > 1$ be odd. We will show a collision under $\chi_n^{(2)}$. Let $\sigma_1 = (1, \alpha, 1, (1, 0)^{\frac{n-3}{2}})$ and $\sigma_2 = (0, \alpha, \alpha^2, (0, \alpha)^{\frac{n-3}{2}})$. Then $\chi_n^{(2)}(\sigma_1) = \chi_n^{(2)}(\sigma_2) = (\alpha, \alpha, 1, (0)^{n-3})$. □

Proof (for $k = 3$:) Let $n > 1$ be odd and $\alpha^3 + \alpha + 1 = 0$. We will show a collision under $\chi_n^{(3)}$. Let $\sigma_1 = (\alpha^3, 1, \alpha, (\alpha^3, 1)^{\frac{n-3}{2}})$ and $\sigma_2 = (\alpha^6, \alpha^4, \alpha^6, (\alpha^6, \alpha^4)^{\frac{n-3}{2}})$. Then $\chi_n^{(3)}(\sigma_1) = \chi_n^{(3)}(\sigma_2) = (\alpha^3, \alpha^2, 0, (\alpha^3)^{n-3})$. □

The remaining cases are open.

It is interesting to see whether for different positive characteristics $\chi_n^{(k)}$ defined similarly is invertible and for which k, n this would be. It turns out, that $\chi_n^{(k)}$ is not invertible over characteristic p for any n, k!

Proposition 13 (**χ_n is not invertible on any field of characteristic p**) *Let $p > 2$ be a prime number. Let n, k be positive integers. Then $\chi_n^{(k)} : \mathbb{F}_{p^k}^n \to \mathbb{F}_{p^k}^n$ is not invertible.*

Proof Take $\sigma = 0^n$ and $\sigma' = (p-2)^n$. Then for any index i, we have $\chi_n^{(k)}(\sigma')_i = \sigma'_i + (\sigma'_{i+1} + 1)\sigma'_{i+2} = p - 2 + (p-1)(p-2) = p \cdot (p-2) \equiv 0 \pmod{p}$. Thus $\chi_n^{(k)}(\sigma') = 0^n = \chi_n^{(k)}(\sigma)$ for all n, k, p. □

References

1. Shair Ahmad, *Cycle structure of automorphisms of finite cyclic groups*, Journal of Combinatorial Theory **6** (1969), no. 4, 370–374.
2. Bertoni, G. and Daemen, J. and Peeters, M. and Van Assche, G., *KECCAK specifications, NIST SHA-3 Submission*, (2008).
3. Eli Biham and Adi Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology **4** (1991), 3–72.
4. Céline Blondeau, Anne Canteaut, and Pascale Charpin, *Differential properties of power functions*, 2010 IEEE International Symposium on Information Theory (2010), 2478–2482.
5. Claude Carlet, Pascale Charpin, and Victor Zinoviev, *Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems*, Designs, Codes and Cryptography **15** (1998), no. 2, 125–156.
6. Carlos Cid, Lorenzo Grassi, Aldo Gunsing, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger, *Influence of the Linear Layer on the Algebraic Degree in SP-Networks*, IACR Transactions on Symmetric Cryptology **2022** (2022), no. 1, 110–137.
7. L. Claesen, J. Daemen, M. Genoe, and G. Peeters, *Subterranean: A 600 Mbit/sec cryptographic VLSI chip*, (1993), 610–613.
8. Joan Daemen, *Cipher and Hash Function Design Strategies based on linear and differential cryptanalysis*, Ph.D. thesis, Katholieke Universiteit Leuven, 1995.
9. Joan Daemen, Alireza Mehrdad, and Silvia Mella, *Computing the Distribution of Differentials over the Non-linear Mapping χ*, Security, Privacy, and Applied Cryptography Engineering (2021), 3–21.
10. Daemen, Joan and Hoffert, Seth and Van Assche, Gilles and Van Keer, Ronny, *The design of Xoodoo and Xoofff*, IACR Transactions on Symmetric Cryptology **2018** (2018), no. 4, 1–38.
11. Daemen, Joan and Massolino, Pedro Maat Costa and Mehrdad, Alireza and Rotella, Yann, *The Subterranean 2.0 Cipher Suite*, IACR Transactions on Symmetric Cryptology **2020** (2020), no. S1, 262–294.
12. Christoph Dobraunig, Yann Rotella, and Jan Schoone, *Algebraic and Higher-Order Differential Cryptanalysis of Pyjamask-96*, IACR Transactions on Symmetric Cryptology **1** (2020), 289–312.
13. Dobraunig, Christoph and Eichlseder, Maria and Grassi, Lorenzo and Lallemand, Virginie and Leander, Gregor and List, Eik and Mendel, Florian and Rechberger, Christian, *Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit*, Advances in Cryptology – CRYPTO 2018 (Cham) (Shacham, Hovav and Boldyreva, Alexandra, ed.), Springer International Publishing, 2018, pp. 662–692.
14. Dobraunig, Christoph and Eichlseder, Maria and Mendel, Florian and Schläffer, Martin, *Ascon v1.2 Submission to NIST*, 2021.
15. Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang, *An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC*, Advances in Cryptology – ASIACRYPT 2020 (Shiho Moriai and Huaxiong Wang, eds.), Springer International Publishing, 2020, pp. 477–506.
16. A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Birkhäuser, 2000.
17. Kurt Hensel, *Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*, Journal für die reine und angewandte Mathematik (1888), no. 129, 68–85.
18. Charles H. Jones, *Generalized hockey stick identities and N-dimensional blockwalking*, Fibonacci Quarterly **34** (1996), 280–288.

19. Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Cambridge University Press, 1996.
20. Fukang Liu, Santanu Sarkar, Willi Meier, and Takanori Isobe, *The Inverse of χ and Its Applications to Rasta-Like Ciphers*, J. Cryptol. **35** (2022), no. 4.
21. Mitsuru Matsui, *Linear cryptanalysis method for des cipher*, International Conference on the Theory and Application of Cryptographic Techniques, 1994.
22. NIST, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Fucntions*, FIPS PUB 202 (2015).
23. ———, *Lightweight Cryptography Standardization Process: NIST Selects Ascon*, 2023.
24. National Bureau of Standards, *Data Encryption Standard, FIPS-Pub.46*, National Bureau of Standards, U.S. Department of Commerce (1977).
25. Ore Öystein, *Contributions to the theory of finite fields*, Transactions of the American Mathematical Society (1934), no. 36, 243–274.
26. Blaise Pascal, *Traité du triangle arithmétique*, Chez Guillaume Desprez (1965).
27. Vincent Rijmen, Paulo S.L.M. Barreto, and Décio L. Gazzoni Filho, *Rotation symmetry in algebraically generated cryptographic substitution tables*, Information Processing Letters **106** (2008), no. 6, 246–250.
28. Jan Schoone and Joan Daemen, *The state diagram of χ*, Cryptology ePrint Archive (2023).
29. Edward Waring, *VII. Problems concerning interpolations*, Philosophical Transactions of the Royal Society (1779), no. 69, 59–67.

7 Appendix

7.1 Proof of Proposition 6

We include here the proof of Proposition 6, since we have not been able to find one in the literature.

Proposition 6 (Differential probabilities for χ [8]) *Let $n > 1$ be an arbitrary odd integer. Let $a' \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b' \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a', b') = 2^{-w(a')}$, where*

$$w(a') = \begin{cases} n-1 & \text{if } a' = 1^n; \\ \mathrm{wt}(a') + r_{a'} & \text{else.} \end{cases}$$

where $r_{a'}$ is the number of 001*-subsequences in a'.*

Proof We can express b' in terms of a' and a (here a is either of the two inputs that together have input difference a') as follows (see [8] Section 6.9):

$$b' = \chi_n(a') + \underbrace{\begin{pmatrix} 0 & a'_2 & a'_1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & a'_3 & a'_2 & \cdots & 0 & 0 \\ 0 & 0 & 0 & a'_4 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a'_{n-1} & a'_{n-2} \\ a'_{n-1} & 0 & 0 & 0 & \cdots & 0 & a'_0 \\ a'_1 & a'_0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}}_{=:D_{a'}} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-3} \\ a_{n-2} \\ a_{n-1} \end{pmatrix} \tag{4}$$

When the differential probability $\mathrm{DP}(a', b') = 2^{-w(a')}$, then the dimension of the kernel of $D_{a'}$ is equal to $n - w(a')$. Therefore the rank of $D_{a'}$ will be equal to $w(a')$.

We will prove this by induction on the Hamming weight of a', which we now denote as k:

$\mathcal{P}(k)$: For all $n > k$ and all $a' \in \mathbb{F}_2^n$ such that $\mathrm{wt}(a') = k$, we have $\mathrm{rk}\, D_{a'} = w(a')$.

We start with the base case $\mathcal{P}(0)$.

Then for any $n > 0$, we have $\mathrm{rk}\, D_{0^n} = 0$ since D_{0^n} is the zero-matrix.

Indeed, $\mathrm{DP}(0, b') = 2^0 = 1$ for all compatible b' (of which there is only $b' = 0$).

The case $\mathcal{P}(1)$ is similar, as we may assume that $a'_0 = 1$ and $a'_i = 0$ for $i \neq 0$. It is immediate that $\mathrm{rk}\, D_{a'} = 2$. When $n \geq 3$, we have $r_{a'} = 1$ and $\mathrm{wt}\, a' = 1$, hence $w(a') = 2 = \mathrm{rk}\, D_{a'}$.

We now explore how we can extend an input difference $a' \in \mathbb{F}_2^{n-2}$ with $\mathrm{wt}\, a' = k$ to an input difference c' with $\mathrm{wt}\, c' = k + 1$. Consider the largest index i for which $a'_i = 1$.

By the shift-invariance of χ_n and the properties of differential probability for linear maps, we can assume that $i = n - 3$.

We can concatenate one of the following to a':

1. 10;
2. 01;
3. $0^\ell 1(0)$.

With (0) we denote that we concatenate another zero if ℓ is even, and do not concatenate it if ℓ is odd. Note that this lists all possibilities to extend an input difference a' to a longer sequence c' with $\mathrm{wt}\, c' = \mathrm{wt}\, a' + 1$.

In each of these three cases we will show that $\mathcal{P}(k + 1)$ is true. Consider some $a' \in \mathbb{F}_2^{n-2}$ such that $\mathrm{wt}\, a' = k$ with $a'_{n-3} = 1$.

1. Let $c' = a' \| 10$ and $d' = a' \| 00$. Both $D_{c'}$ and $D_{d'}$ are $n \times n$ matrices. By the induction hypothesis, we know that $\mathrm{rk}\, D_{d'} = \mathrm{wt}\, d' + r_{d'}$. We make a case distinction:
   a. Either d' starts with $0^l 1$ for $l > 1$;
   b. or d' starts with 01;
   c. or d' starts with 1.

   We now assume each of these cases separately.
   a. We have $\mathrm{wt}\, c' = \mathrm{wt}\, d' + 1$ and $r_{c'} = r_{d'}$. Thus, we have to show that $\mathrm{rk}\, D_{c'} = \mathrm{rk}\, D_{d'} + 1$. For that, we consider the following submatrix of $D_{a'}$:

$$\mathrm{sub}\,.D_{a'} := \begin{matrix} a'_{n-3} & a'_{n-4} & 0 & 0 \\ 0 & a'_{n-2} & a'_{n-3} & 0 \\ 0 & 0 & a'_{n-1} & a'_{n-2} \\ 0 & 0 & 0 & a'_0 \end{matrix}$$

   We then note that all other coordinates of $D_{a'}$ do not change when we go from $D_{d'}$ to $D_{c'}$. We have:

	a'_{n-4}	a'_{n-3}	a'_{n-2}	a'_{n-1}	a'_0
c' :	?	1	1	0	0
d' :	?	1	0	0	0

   The given columns are extended upwards and downwards with 0s in the matrix $D_{a'}$. The same holds for the rows, that are extended leftwards with

0s, except for the last one, which has a'_{n-1} in its first position. There we, thus, have

$$\operatorname{sub}.D_{d'} := \begin{matrix} 1 & a'_{n-4} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix} \qquad \operatorname{sub}.D_{c'} := \begin{matrix} 1 & a'_{n-4} & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{matrix}$$

In this forelying case, $a'_{n-1} = 0$, hence this submatrix is independent on the other blocks in $D_{a'}$. It is immediately clear by looking at the first three rows of the submatrices, that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 1$.

b. This case is identical to 1a.

c. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$ and $r_{c'} = r_{d'} - 1$. Thus, we have to show that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'}$. We have:

	a'_{n-4}	a'_{n-3}	a'_{n-2}	a'_{n-1}	a'_0
c' :	?	1	1	0	1
d' :	?	1	0	0	1

and thus

$$\operatorname{sub}.D_{d'} := \begin{matrix} 1 & a'_{n-4} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \qquad \operatorname{sub}.D_{c'} := \begin{matrix} 1 & a'_{n-4} & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{matrix}$$

wherefrom it is clear that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'}$.

Therefore, case 1. has been shown.

2. Let $c' = a' \| 01$ and $d' = a' \| 00$. The case starts similar as case 1:
   a. Either d' starts with $0^l 1$ for $l > 1$;
   b. or d' starts with 01;
   c. or d' starts with 1.

   We now assume each of these cases separately.

   a. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$ and $r_{c'} = r_{d'}$. Thus, we have to show that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 1$.
   Here we concern ourselves with the 'submatrix':

$$\operatorname{sub}.D_{a'} := \begin{matrix} 0 & 0 & a'_{n-3} & 0 \\ 0 & 0 & a'_{n-1} & a'_{n-2} \\ a'_{n-1} & 0 & 0 & a'_0 \\ a'_1 & a'_0 & 0 & 0 \end{matrix}$$

We then note that all other coordinates of $D_{a'}$ do not change when we go from $D_{d'}$ to $D_{c'}$. We have:

	a'_{n-3}	a'_{n-2}	a'_{n-1}	a'_0	a'_1
c' :	1	0	1	0	0
d' :	1	0	0	0	0

We write the 'submatrices' of $D_{d'}$ and $D_{c'}$ and immediately see that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 1$:

$$\text{sub}.D_{d'} := \begin{matrix} 0&0&1&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{matrix} \qquad \text{sub}.D_{c'} := \begin{matrix} 0&0&1&0 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&0&0&0 \end{matrix}$$

b. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$ and $r_{c'} = r_{d'} - 1$. Thus, we have to show $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'}$. We have:

$$\begin{array}{cccccc} & a'_{n-3} & a'_{n-2} & a'_{n-1} & a'_0 & a'_1 \\ c': & 1 & 0 & 1 & 0 & 1 \\ d': & 1 & 0 & 0 & 0 & 1 \end{array}$$

We take the same submatrices for $D_{c'}$ and $D_{d'}$:

$$\text{sub}.D_{d'} := \begin{matrix} 0&0&1&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 1&0&0&0 \end{matrix} \qquad \text{sub}.D_{c'} := \begin{matrix} 0&0&1&0 \\ 0&0&1&0 \\ 1&0&0&0 \\ 1&0&0&0 \end{matrix}$$

We easily see that matrices $D_{c'}$ and $D_{d'}$ have equal rank.

c. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$ and $r_{c'} = r_{d'} - 1$. Thus, we have to show $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'}$. We have:

$$\begin{array}{cccccc} & a'_{n-3} & a'_{n-2} & a'_{n-1} & a'_0 & a'_1 \\ c': & 1 & 0 & 1 & 1 & ? \\ d': & 1 & 0 & 0 & 1 & ? \end{array}$$

Then

$$\text{sub}.D_{d'} := \begin{matrix} 0&0&1&0 \\ 0&0&0&0 \\ 0&0&0&1 \\ ?&1&0&0 \end{matrix} \qquad \text{sub}.D_{c'} := \begin{matrix} 0&0&1&0 \\ 0&0&1&0 \\ 1&0&0&1 \\ ?&1&0&0 \end{matrix}$$

It is immediately clear that the ranks of the submatrices are equal for $D_{d'}$ and $D_{c'}$, hence $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'}$.

Therefore, case 2. has been shown.

3. Let $c' = a' \| 0^\ell 1(0)$ and $d' = a' \| 0^\ell 0(0)$. Both $D_{c'}$ and $D_{d'}$ are $(n+\ell) \times (n+\ell)$ matrices. By the induction hypothesis, we know that $\operatorname{rk} D_{d'} = \operatorname{wt} d' + r_{d'}$. We make a case distinction:
   a. Either d' starts with $0^l 1$ for $l > 1$;
   b. or d' starts with 01;
   c. or d' starts with 1.

   We now assume each of these cases separately.

   a. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$ and $r_{c'} = r_{d'} + 1$. Therefore, we need to show that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 2$. We make a case distinction for whether ℓ is even or odd.

i. ℓ is odd, hence we do not need to add the last (0). Set $m = \ell + n$. Consider the following values:

$$\begin{array}{cccccc} & a'_{m-3} & a'_{m-2} & a'_{m-1} & a'_0 & a'_1 \\ c': & 0 & 0 & 1 & 0 & 0 \\ d': & 0 & 0 & 0 & 0 & 0 \end{array}$$

By considering the following submatrix of $D_{a'}$,

$$\operatorname{sub}.D_{a'} := \begin{matrix} 0 & a'_{m-2} & a'_{m-3} & 0 \\ 0 & 0 & a'_{m-1} & a'_{m-2} \\ a'_{m-1} & 0 & 0 & a'_0 \\ a'_1 & 0 & 0 & 0 \end{matrix},$$

and by filling it in, it is immediately clear that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 2$.

ii. Set $m = \ell + n$. We considering the following values:

$$\begin{array}{cccccc} & a'_{m-4} & a'_{m-3} & a'_{m-2} & a'_{m-1} & a'_0 \\ c': & 0 & 0 & 1 & 0 & 0 \\ d': & 0 & 0 & 0 & 0 & 0 \end{array}$$

By considering the following submatrix of $D_{a'}$,

$$\operatorname{sub}.D_{a'} := \begin{matrix} a'_{n-3} & a'_{n-4} & 0 & 0 \\ 0 & a'_{n-2} & a'_{n-3} & 0 \\ 0 & 0 & a'_{n-1} & a'_{n-2} \\ 0 & 0 & 0 & a'_0 \end{matrix},$$

it is again immediately clear that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 2$, as required.

b. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$. We immediately have to make a case distinction to whether ℓ is even or odd. Set $m = n + \ell$.

i. If ℓ is odd, then a'_{m-1} flips. We then have $r'_c = r'_d$, so we have to show $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 1$. Hence, we consider the following values:

$$\begin{array}{cccccc} & a'_{m-3} & a'_{m-2} & a'_{m-1} & a'_0 & a'_1 \\ c': & 0 & 0 & 1 & 0 & 1 \\ d': & 0 & 0 & 0 & 0 & 1 \end{array}$$

We then consider the following submatrix:

$$\operatorname{sub}.D_{a'} := \begin{matrix} 0 & a'_{m-2} & a'_{m-3} & 0 \\ 0 & 0 & a'_{m-1} & a'_{m-2} \\ a'_{m-1} & 0 & 0 & a'_0 \\ a'_1 & 0 & 0 & 0 \end{matrix}$$

We see that the rank of $D_{c'}$ is one higher than the rank of $D_{d'}$, as required.

$$\begin{array}{cccccc} & a'_{m-4} & a'_{m-3} & a'_{m-2} & a'_{m-1} & a'_0 \\ c': & 0 & 0 & 1 & 0 & 0 \\ d': & 0 & 0 & 0 & 0 & 0 \end{array}$$

ii. In this case $a'_{m-1} = 0$ in c' and d', but a'_{m-2} changes. Hence we have $r_{c'} = r_{d'} + 1$, and we need to show that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 2$. Consider the following values:
By considering the submatrix

$$\text{sub}\,.D_{a'} := \begin{matrix} 0 & a'_{m-4} & 0 & 0 \\ 0 & a'_{m-2} & a'_{m-3} & 0 \\ 0 & 0 & a'_{m-1} & a'_{m-2} \\ a'_{m-1} & 0 & 0 & a'_0 \end{matrix},$$

we immediately obtain that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'}$.

c. We have $\operatorname{wt} c' = \operatorname{wt} d' + 1$ and $r_{c'} = r_{d'}$. We therefore need to show that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 1$. As before, we make a case distinction:

i. Let ℓ be even and consider

$$\begin{array}{cccccc} & a'_{m-4} & a'_{m-3} & a'_{m-2} & a'_{m-1} & a'_0 \\ c': & 0 & 0 & 1 & 0 & 1 \\ d': & 0 & 0 & 0 & 0 & 1 \end{array}$$

Then, we consider the submatrix

$$\text{sub}\,.D_{a'} := \begin{matrix} a'_{m-3} & a'_{m-4} & 0 & 0 \\ 0 & a'_{m-2} & a'_{m-3} & 0 \\ 0 & 0 & a'_{m-1} & a'_{m-2} \\ 0 & 0 & 0 & a'_0 \end{matrix}$$

and fill in the values for $D_{d'}$ and $D_{c'}$:

$$\text{sub}\,.D_{d'} := \begin{matrix} 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,1 \end{matrix} \qquad \text{sub}\,.D_{c'} := \begin{matrix} 0\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,1 \\ 0\,0\,0\,1 \end{matrix}$$

From this, we see that $\operatorname{rk} D_{c'} = \operatorname{rk} D_{d'} + 1$.

ii. Assume that ℓ is odd and consider

$$\begin{array}{cccccc} & a'_{m-3} & a'_{m-2} & a'_{m-1} & a'_0 & a'_1 \\ c': & 0 & 0 & 1 & 1 & ? \\ d': & 0 & 0 & 0 & 1 & ? \end{array}$$

We consider the submatrix of $D_{a'}$ given by:

$$\text{sub}\,.D_{a'} := \begin{matrix} 0 & a'_{m-2} & a'_{m-3} & 0 \\ 0 & 0 & a'_{m-1} & a'_{m-2} \\ a'_{m-1} & 0 & 0 & a'_0 \\ a'_1 & 0 & 0 & 0 \end{matrix}$$

and fill in the values for $D_{d'}$ and $D_{c'}$:

$$\text{sub}.D_{d'} := \begin{matrix} 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,1 \\ ?\,0\,0\,0 \end{matrix} \qquad \text{sub}.D_{c'} := \begin{matrix} 0\,0\,0\,0 \\ 0\,0\,1\,0 \\ 1\,0\,0\,1 \\ ?\,0\,0\,0 \end{matrix}$$

From this, we see that, independently of the value of ?, that the rank increase when going from $D_{d'}$ to $D_{c'}$.

Therefore, case 3. has been shown.

By the above case distinction, we have proven half of the proposition by means of induction.

For the other half, namely that $w(a') = n - 1$, when $a' = 1^n$, we just need to show that the rank of $D_{a'} = n - 1$. This follows by doing elementary row reductions. The echelon form will consist of an $(n - 1) \times (n - 1)$ identity matrix I_{n-1}, with an $(n - 1) \times 1$ all-one column to the right of it, and an all-zero row below all this:

$$\begin{pmatrix} & & & 1 \\ & I_{n-1} & & \vdots \\ & & & 1 \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

and the result follows. □

7.2 Actual sparsity and degree

Here, we list the actual numbers for the minimum sparsity, maximum sparsity, minimum degree and maximum degree for univariate representations of χ_n for several n.

Below those, we also give tables for the exact different univariate representations for χ_n.

	Min. sparsity	Max. sparsity	Min. degree	Max. degree
$n = 3$	1	3	6	6
$n = 5$	5	9	18	24
$n = 7$	11	19	64	96
$n = 9$	15	33	258	384

Table 8 The true bounds on sparsity and degree for univariate expressions for χ_n.

In the following tables for χ_3, χ_5, χ_7, we see $S_n := \text{Sym}(\{1, \ldots, n\})$, instead of $\{0, \ldots, n - 1\}$.

In Table 11, we write for the normal element a set of non-negative integers. These denote the exponents of the monomials that have coefficient 1 in the defining polynomial of the normal element. For instance, $\{7, 6, 5, 2, 0\}$ denotes $\beta^7 + \beta^6 + \beta^5 + \beta^2 + 1 = 0$.

Similarly, we write a tuple of non-negative integers for the resulting polynomials.

normal element	iso. (σ)	resulting polynomial
$\beta^3+\beta^2+1=0$	id	t^6
	(2 3)	$t^6+t^4+t^2$

Table 9 Univariate representations of χ_3.

normal element	iso. (σ)	resulting polynomial
$\beta^5+\beta^4+\beta^2+\beta+1=0$	id	$t^{20}+t^{12}+t^8+t^6+t^5+t^4+t^3$
	(2 3 5 4)	$t^{18}+t^{17}+t^{10}+t^6+t^5$
	(2 4 5 3)	$t^{20}+t^{16}+t^{12}+t^{10}+t^5+t^4+t^3+t^2+t$
	(2 5)(3 4)	$t^{24}+t^{17}+t^9+t^8+t^5+t^4+t^3$
$\beta^5+\beta^4+\beta^3+\beta+1=0$	id	$t^{24}+t^{18}+t^{17}+t^{16}+t^4+t^3+t$
	(2 3 5 4)	$t^{24}+t^{20}+t^{16}+t^{10}+t^9+t^8+t^5+t^4+t^2$
	(2 4 5 3)	$t^{20}+t^{18}+t^{17}+t^{10}+t^9+t^8+t^2$
	(2 5)(3 4)	$t^{24}+t^{20}+t^{12}+t^6+t^2$
$\beta^5+\beta^4+\beta^3+\beta^2+1=0$	id	$t^{24}+t^{10}+t^9+t^6+t^5+t^2+t$
	(2 3 5 4)	$t^{20}+t^{17}+t^{12}+t^8+t^4+t^3+t$
	(2 4 5 3)	$t^{24}+t^9+t^8+t^6+t^4+t^3+t$
	(2 5)(3 4)	$t^{18}+t^{17}+t^{16}+t^{10}+t^9+t^6+t^4+t^2+t$

Table 10 Univariate representations of χ_5.

normal element	iso. (σ)	resulting polynomial
$\{7, 6, 5, 2, 0\}$	id	$(96, 80, 68, 48, 40, 34, 33, 32, 24, 18, 16, 12, 9, 8, 2)$
	(2 3 5)(4 7 6)	$(80, 66, 48, 40, 33, 32, 24, 20, 12, 10, 9, 4, 1)$
	(2 4 3 7 5 6)	$(96, 68, 66, 65, 48, 36, 34, 32, 24, 18, 9, 8, 4)$
	(2 5 3)(4 6 7)	$(96, 72, 65, 64, 36, 32, 18, 17, 16, 10, 9, 8, 6, 4, 3)$
	(2 6 5 7 3 4)	$(80, 68, 40, 33, 24, 20, 12, 10, 6, 5, 4, 2, 1)$
	(2 7)(3 6)(4 5)	$(96, 72, 66, 65, 64, 36, 18, 17, 16, 10, 8, 6, 5, 4, 3)$
$\{7, 6, 4, 2, 0\}$	id	$(96, 80, 72, 68, 66, 64, 36, 34, 32, 20, 9, 8, 6, 3, 1)$
	(2 3 5)(4 7 6)	$(96, 80, 40, 34, 32, 24, 20, 18, 16, 10, 8, 6, 2)$
	(2 4 3 7 5 6)	$(96, 80, 48, 32, 24, 18, 17, 9, 6, 5, 3)$
	(2 5 3)(4 6 7)	$(96, 72, 68, 66, 65, 64, 36, 24, 20, 12, 8, 4, 3)$
	(2 6 5 7 3 4)	$(64, 48, 40, 20, 17, 12, 10, 9, 8, 5, 3)$
	(2 7)(3 6)(4 5)	$(72, 68, 64, 48, 36, 34, 33, 24, 20, 18, 6, 5, 1)$
$\{7, 6, 4, 1, 0\}$	id	$(96, 80, 66, 48, 40, 36, 33, 24, 18, 12, 10, 6, 5, 4, 2$
	(2 3 5)(4 7 6)	$(96, 68, 66, 65, 48, 40, 36, 34, 32, 24, 20, 18, 12, 4, 3, 2, 1)$
	(2 4 3 7 5 6)	$(80, 72, 68, 65, 34, 33, 10, 8, 5, 3, 2)$
	(2 5 3)(4 6 7)	$(66, 64, 40, 34, 32, 20, 18, 12, 9, 6, 5, 4, 1)$
	(2 6 5 7 3 4)	$(96, 65, 48, 34, 33, 24, 20, 18, 17, 12, 10, 9, 6, 4, 2)$
	(2 7)(3 6)(4 5)	$(96, 80, 66, 65, 48, 40, 34, 32, 20, 17, 16, 10, 8, 6, 5, 4, 3, 2, 1)$
$\{7, 6, 3, 1, 0\}$	id	$(80, 64, 40, 34, 33, 32, 24, 20, 18, 12, 10, 8, 4, 3, 2)$
	(2 3 5)(4 7 6)	$(80, 68, 48, 36, 33, 24, 18, 16, 12, 10, 6, 4, 3)$
	(2 4 3 7 5 6)	$(68, 65, 64, 34, 33, 32, 24, 18, 17, 10, 5, 4, 1)$
	(2 5 3)(4 6 7)	$(96, 72, 68, 64, 40, 20, 18, 16, 9, 8, 6, 5, 2)$
	(2 6 5 7 3 4)	$(80, 65, 64, 40, 34, 24, 18, 16, 12, 9, 8, 6, 5, 4, 3, 2, 1)$
	(2 7)(3 6)(4 5)	$(96, 80, 66, 65, 64, 33, 32, 24, 18, 17, 16, 10, 8, 5, 1)$
$\{7, 6, 0\}$	id	$(96, 68, 65, 64, 48, 36, 34, 33, 32, 20, 16, 12, 10, 6, 5, 4, 3, 2, 1)$
	(2 3 5)(4 7 6)	$(72, 68, 66, 65, 64, 48, 40, 34, 32, 20, 18, 17, 10, 8, 6, 5, 4, 3, 2)$
	(2 4 3 7 5 6)	$(80, 68, 48, 40, 36, 33, 32, 24, 20, 17, 16, 8, 5, 3, 2)$
	(2 5 3)(4 6 7)	$(96, 80, 68, 66, 65, 33, 32, 20, 18, 17, 12, 5, 4)$
	(2 6 5 7 3 4)	$(96, 72, 66, 65, 64, 36, 34, 33, 32, 24, 20, 17, 10, 9, 5, 3, 2)$
	(2 7)(3 6)(4 5)	$(96, 80, 48, 40, 36, 34, 33, 32, 24, 18, 16, 12, 10, 6, 3)$
$\{7, 6, 5, 3, 2, 1, 0\}$	id	$(80, 64, 48, 40, 36, 32, 24, 20, 16, 12, 10, 8, 5, 4, 3)$
	(2 3 5)(4 7 6)	$(68, 65, 36, 34, 33, 24, 20, 18, 17, 12, 9, 6, 5, 4, 3)$
	(2 4 3 7 5 6)	$(80, 66, 40, 36, 34, 33, 18, 17, 16, 10, 5, 4, 3, 2, 1)$
	(2 5 3)(4 6 7)	$(72, 68, 66, 40, 33, 20, 17, 16, 12, 10, 9, 5, 1)$
	(2 6 5 7 3 4)	$(96, 80, 72, 68, 66, 65, 64, 34, 18, 17, 16, 12, 10, 9, 6, 4, 3, 2, 1)$
	(2 7)(3 6)(4 5)	$(96, 80, 66, 65, 64, 40, 34, 33, 32, 24, 8, 5, 3)$
$\{7, 6, 5, 4, 2, 1, 0\}$	id	$(66, 64, 48, 40, 36, 34, 33, 18, 16, 12, 6, 5, 4)$
	(2 3 5)(4 7 6)	$(96, 80, 66, 65, 48, 34, 20, 18, 12, 10, 9, 8, 4, 2, 1)$
	(2 4 3 7 5 6)	$(80, 72, 66, 65, 36, 34, 32, 24, 17, 8, 5, 3, 1)$
	(2 5 3)(4 6 7)	$(96, 68, 66, 64, 34, 32, 20, 17, 12, 10, 9, 8, 6)$
	(2 6 5 7 3 4)	$(96, 68, 48, 40, 33, 24, 17, 16, 10, 9, 6, 5, 2)$
	(2 7)(3 6)(4 5)	$(96, 66, 48, 40, 34, 32, 20, 18, 17, 10, 8, 3, 2)$

Table 11 Univariate representations of χ_7.