Threshold implementations of cryptographic functions between finite Abelian groups

Enrico Piccione

University of Bergen, Bergen, Norway enrico.piccione@uib.no

Abstract. The threshold implementation technique has been proposed in 2006 by Nikova et al. as a countermeasure to mitigate cryptographic side-channel attacks on hardware implementations when the effect of glitches is taken into account. This technique is based on Boolean sharing (also called masking) and it was developed for securing symmetric ciphers such as AES. In 2023, Piccione et al. proposed a general construction of threshold implementations that is universal for S-boxes that are bijective vectorial Boolean function (functions from a binary vector space $\mathbb{F}_2^n$ into itself). In this paper, we further generalize the construction and we propose a general theory of threshold implementations for any type of S-boxes. We investigate the case of functions (also not necessarily bijective) that are defined between two finite Abelian groups and we use the definition of threshold implementation given by Dhooghe et al. in 2019 with additive sharing. To show that this generalized notion is as useful as the one for Boolean sharing, we prove that many classical results still hold. An important tool in this theory is the notion of functional degree introduced by Aichinger and Moosbauer in 2021 which generalizes the algebraic degree of a vectorial Boolean function. We show that if F has functional degree (at most) d and the cardinality of the domain is divisible by the cardinality of the codomain, then F admits a threshold implementation $\mathcal{F}$ with $s \geq d+2$ shares in input and $d+2$ shares in output. Moreover, we provide a complete overview on which are the available tools for studying the functional degree and how to represent those functions using a Integer-Valued (IV) polynomial representation. Then we apply our theory for the following applications: defining the inner product masking in our setting, providing a threshold implementation of any multiplication map, and computing the functional degree and the IV polynomial representations of the conversion maps between $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$.

Keywords: No keywords given.

1 Introduction

Differential Power Analysis (DPA) attacks [KJJ99] target the hardware implementations of a cryptographic algorithm by measuring the power consumption of the physical device. Since then, many countermeasures were developed in order to mitigate those attacks. One of the most common is called *Boolean masking* [GP99, CJRR99] which is a technique based on *Boolean sharing* that secure the implementation against a formally defined adversary model. However, if the effect of glitches is not taken into account this can lead to an attack on a masked implementation [MPO05]. Nikova, Rechberger, and Rijmen [NRR06] published in 2006 a countermeasure called *Threshold Implementation* (TI) which builds upon Boolean masking and takes glitches into account.

In mathematical terms, a threshold implementation is a vectorial Boolean function $\mathcal{F}$ that satisfies three fundamental properties with respect to a given vectorial Boolean function F. Those properties are correctness, non-completeness, and uniformity. Throughout the

years, the problem of constructing $\mathcal{F}$ for a given F was considered a challenging problem [BNN+12, BGN+15, BBS17]. In [PAB+23], this has been solved for the case where F is bijective but with $d+2$ shares where d is the algebraic degree of F. The theoretical optimal number is $d+1$, but there is some evidence reported in [BNN+12, PAB+23] to the fact that for many functions F the number of optimal shares is actually $d+2$ with one example for which it is mathematically proven. In this paper, we do not discuss the case $d+1$ further and, instead, we consider a more general mathematical setting where we can further generalize the construction in [PAB+23]. With this, we provide a better understanding of the threshold implementation theory. We consider the problem of constructing a threshold implementation for a function $F\colon \mathbb{X} \to \mathbb{Y}$ between two finite Abelian groups $\mathbb{X}$ and $\mathbb{Y}$ where we use the definition provided by Dhooghe et al. [DNR19] with *additive sharing* both in the input and the output. For any $x \in \mathbb{X}$ (resp. $y \in \mathbb{Y}$), a vector of shares $(x_1, \dots, x_s) \in \mathbb{X}^s$ (resp. $(y_1, \dots, y_t) \in \mathbb{Y}^t$) is such that $x_1 + \cdots + x_s = x$ (resp. $y_1 + \cdots + y_s = y$). The additive sharing over $\mathbb{Z}_{2^n}$ is called *arithmetic sharing* (or *arithmetic masking*) [Gou01] and it has been the building block of the implementations of two of the NIST standards for post quantum cryptography Kyber and Dilithium [Bou22]. Moreover, there has been a recent interest in *prime-field sharing* (also called *prime-field masking*) over Mersenne primes $2^n - 1$ [CMM+23] which is the additive sharing over $\mathbb{F}_{2^n-1}$.

A fundamental notion in the threshold implementation theory is the one of algebraic degree. For functions between Abelian groups, we are going to use the notion of *functional degree*. Aichinger and Moosbauer in [AM21] introduce such notion with the purpose of extending Chevalley-waring type results to the general case of a function $F\colon \mathbb{X} \to \mathbb{Y}$ between two Abelian groups $\mathbb{X}$ and $\mathbb{Y}$. The functional degree of F is defined by the smallest positive natural number such that Fréchet's equation is satisfied, which is equivalent to ask that every $d+1$-th order derivative vanishes. A derivative of F through a direction $a \in \mathbb{X}$ is defined by $\Delta_a F(x) = F(x+a) - F(x)$ for any $x \in \mathbb{X}$. The idea of using Fréchet's equation to introduce a notion of degree was already studied by many authors in the past (see for instance [Lac04]). However, we refer to the paper [AM21] because this is the first work that gives solid mathematical foundations without the use of any representation of F. We also present an overview of the following works [Sch14, CS22] which have studied the Integer-Valued (IV) polynomial representation of functions with finite functional degree. We believe that this representation could be useful for cryptographic application in the case where a polynomial representation is not possible.

As main result of this paper, we provide a threshold implementation $\mathcal{F}$ with $s \geq d+2$ shares in input and $d+2$ shares in output for any $F\colon \mathbb{X} \to \mathbb{Y}$ with functional degree at most $d < \infty$ and such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. In particular, the result holds for any vectorial Boolean function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m \leq n$ and F having algebraic degree at most d. Such construction allows the implementation of F in hardware by only using the arithmetic of the group. After that, we discuss some applications. We generalize in a simple way the *inner product sharing* [BFG15] and we show that any result we have achieved for additive sharing still holds. We provide a threshold implementation with 4 shares of the multiplication map over a finite ring. We compute the functional degree and the IV polynomial representation of the conversion map $\mathbb{F}_p^n \to \mathbb{Z}_{p^n}$ and of its inverse. We prove that both of them can be implemented with $n+2$ shares.

2 Preliminaries

An Abelian group is a non-empty set $\mathbb{X}$ with an operation "+" such that it is associative, it is commutative, there exists an identity element $0 \in \mathbb{X}$, and every element has an inverse. A ring is a non-empty set with two operations "+" and "$\cdot$" such that they are distributive, R is an Abelian group with respect to the addition, the multiplication is associative, and there exists an identity element $1 \in R$ with respect to the multiplication. Observe that we

did not impose that $1 \neq 0$ because we want that $R = \{0\}$ is still a ring. Indeed, if $1 = 0$ then $r = r \cdot 1 = r \cdot 0 = 0$ for all $r \in R$. A field is a non-empty set $\mathbb{F}$ that is a ring and such that $\mathbb{F} \setminus \{0\}$ is an Abelian group with respect to the multiplication.

We denote by $\mathbb{N}$ the natural numbers greater or equal than zero, as $\mathbb{Z}$ the integer, and as $\mathbb{Q}$ the rational numbers. For any $n \in \mathbb{N}$ with $n \geq 2$, we denote by $\mathbb{Z}_n$ the ring of integers modulo n and we usually represent them as integers between 0 and $n-1$ or as classes $a + n\mathbb{Z} = \{a + bn \colon b \in \mathbb{Z}\}$ for any $a \in \mathbb{Z}$. Moreover, we use the notation $\mathbb{Z}_0 = \mathbb{Z}$ and $\mathbb{Z}_1 = \{0\}$. By our definition, $\mathbb{Z}_1$ is still a ring. Let q be the power of a prime number p, then we denote by $\mathbb{F}_q$ the finite field with q elements. We recall that $\mathbb{F}_p = \mathbb{Z}_p$ and that $\mathbb{F}_q \neq \mathbb{Z}_q$ if $q \neq p$.

Let $s, t \in \mathbb{N}$. We define $[t, s] = \{i \in \mathbb{N} \colon t \leq i \leq s,\, i \geq 1\}$, $[s] = [1, s]$ (notice that $[0] = \emptyset$), $\mathcal{P}_s = \{I \colon I \subseteq [s]\}$, and $\mathcal{P}_s^* = \mathcal{P}_s \setminus \{[s]\}$ (notice that $\mathcal{P}_0 = \{\emptyset\}$). Moreover, for any $j \in \{0, \ldots, s\}$, we write $\mathcal{P}_{s,j} = \{I \in \mathcal{P}_s \mid |I| = j\}$ (notice that $\mathcal{P}_{s,0} = \mathcal{P}_0$).

In this paper, we consider every Abelian group $\mathbb{X}$ with additive notation. Let $x_1, \ldots, x_s \in \mathbb{X}$, then we use the convention that $\sum_{i \in [0]} x_i = 0$. For every $x \in \mathbb{X}$ and $n \in \mathbb{Z}$ we will write $nx = \sum_{i \in [n]} x$ if $n \geq 0$ and $nx = -((-n)x)$ if $n < 0$. An homomorphism is a map $\phi \colon \mathbb{X} \to \mathbb{Y}$ between two Abelian groups $\mathbb{X}$ and $\mathbb{Y}$ such that $\phi(x + x') = \phi(x) + \phi(x')$ for any $x, x' \in \mathbb{X}$. We say that $\mathbb{X}$ and $\mathbb{Y}$ are isomorphic if there exists a bijective homomorphism between them. We say that $\mathbb{X}$ is finitely generated if there exists a finite set $A = \{a_1, \ldots, a_k\} \subseteq \mathbb{X}$ such that $\mathbb{X} = \{\sum_{i \in [k]} n_i a_i \colon n_i \in \mathbb{Z}\}$. If such A exists of cardinality 1, then $\mathbb{X}$ is called cyclic. Every cyclic group $\mathbb{X}$ is isomorphic to $\mathbb{Z}_n$. Indeed, if $\mathbb{X}$ is finite then $n = |\mathbb{X}|$ and otherwise $n = 0$ which means that $\mathbb{X}$ is isomorphic to the ring of integers $\mathbb{Z}_0 = \mathbb{Z}$. Every finitely generated Abelian group is isomorphic to a Cartesian product of the form $\prod_{i \in [n]} \mathbb{Z}_{q_i}$ for some $q_i \in \mathbb{N}$. Moreover, one can assume that q_i is either 0, 1, or a prime power.

For any $k \in \mathbb{N}$ with $k \geq 2$, the k-adic expansion of a natural number $a \in \mathbb{N}$ is its representation as the series

$$a = \sum_{i=1}^{\infty} a_i k^{i-1}$$

where each a_i is an integer between 0 and $k-1$. If it is clear from the context that $a < k^n$ for some $n \in \mathbb{N}$, we will say that its k-adic expansion is the truncated sum $a = \sum_{i \in [n]} a_i k^{i-1}$.

We recall that the notions of "sup" and "inf" coincide respectively with the ones of "max" and "min" when they are applied on finite subsets of $\mathbb{N}$. We will use the conventions that $\inf(\emptyset) = \sup(\emptyset) = 0$ and for every $A \subseteq \mathbb{N}$ that has infinite cardinality we have $\sup(A) = \infty$.

2.1 Functions between Abelian groups

Let $F \colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups.

We say that F is a linear function if it is a group homomorphism between $\mathbb{X}$ and $\mathbb{Y}$, that is $F(x + x') = F(x) + F(x')$ for all $x, x' \in \mathbb{X}$. We say that F is an affine function if $F' = F - F(0)$ is a linear function. We will use the terms *linear* and *affine* even though $\mathbb{X}$ and $\mathbb{Y}$ are not necessarily vector or affine spaces. We define the *derivative* of F in $a \in \mathbb{X}$ as the function $\Delta_a F(x) = F(x + a) - F(x)$ for any $x \in \mathbb{X}$ and the *k-th order derivative* of F in $\underline{a} = (a_1, \ldots, a_k) \in \mathbb{X}^k$ as the function

$$\Delta_{\underline{a}}^{(k)} F = \Delta_{a_1} \Delta_{a_2} \cdots \Delta_{a_k} F.$$

If $\mathbb{X} = \mathbb{Z}_n$, we denote $\Delta = \Delta_1$ and $\Delta^{(k)} = \Delta_{(1,\ldots,1)}^{(k)}$ where $1 \in \mathbb{Z}_n$. In some cases, we will use the lower case letter f to denote a function from an Abelian group $\mathbb{X}$ to a cyclic group $\mathbb{Y} = \mathbb{Z}_q$ where q is a prime power.

Let $\mathbb{X}_1, \ldots, \mathbb{X}_n, \mathbb{Y}_1, \ldots, \mathbb{Y}_m$ be Abelian groups. Let $F\colon \prod_{i\in[n]} \mathbb{X}_i \to \prod_{j\in[m]} \mathbb{Y}_j$. For any $x \in \prod_{i\in[n]} \mathbb{X}_i$, we can write

$$F(x) = (F_1(x), \ldots, F_m(x))$$

where $F_j\colon \prod_{i\in[n]} \mathbb{X}_i \to \mathbb{Y}_j$ for any $j \in [m]$. Let $i \in [n]$, we define the *partial derivative* of F in $a \in \mathbb{X}_i$ through the direction of the i-th coordinate as the function $\partial_a^i F\colon \prod_{i\in[n]} \mathbb{X}_i \to \prod_{j\in[m]} \mathbb{Y}_j$ defined by

$$\partial_a^i F(x) = F(x_1, \ldots, x_i + a, \ldots, x_n) - F(x)$$

for any $x = (x_1, \ldots, x_n) \in \prod_{i\in[n]} \mathbb{X}_i$ and the *k-th order partial derivative* of F in $\underline{a} = (a_1, \ldots, a_k) \in (\mathbb{X}_i)^k$ as the function

$$\partial_{\underline{a}}^{i,(k)} F = \partial_{a_1}^i \partial_{a_2}^i \cdots \partial_{a_k}^i F.$$

We say that the function F depends on its i-th coordinate input if there exists $a \in \mathbb{X}$ such that $\partial_a^i F \neq 0$. Similarly as before, if $\mathbb{X}_i = \mathbb{Z}_{m_i}$, we denote $\partial^i = \partial_1^i$ and $\partial^{i,(k)} = \partial_{(1,\ldots,1)}^{i,(k)}$ where $1 \in \mathbb{Z}_{m_i}$. Moreover, for any $\underline{k} = (k_1, \ldots, k_n) \in \mathbb{N}^n$, we denote

$$\partial^{(\underline{k})} = \partial^{1,k_1} \cdots \partial^{1,k_n}.$$

In some cases, we will use the calligraphic letter $\mathcal{F}$ to denote a function from $\mathbb{X}^s$ to $\mathbb{Y}^t$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups.

Suppose that $\mathbb{X}$ and $\mathbb{Y}$ are finite Abelian groups. We say that F is balanced if $|F^{-1}(y)| = |\mathbb{X}|/|\mathbb{Y}|$ for any $y \in \mathbb{Y}$. Observe that if F is balanced and $|\mathbb{X}| = |\mathbb{Y}|$, then F is bijective.

2.2 Algebraic degree of functions between finite-dimensional vector spaces over $\mathbb{F}_p$ and their representation

A function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is called a Boolean function and a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a vectorial Boolean function.

Let p be a prime. Any function F between finite-dimensional vector spaces over $\mathbb{F}_p$ can be represented as a vectorial function $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ and it has a unique representation of the following form

$$F(x_1, \ldots, x_n) = \sum_{\underline{u}\in\{0,\ldots,p-1\}^n} c_{\underline{u}} x_1^{u_1} \cdots x_n^{u_n}, \quad c_{\underline{u}} \in \mathbb{F}_p^m \tag{1}$$

which is called the *algebraic normal form (ANF)*. The *algebraic degree* of F is defined by

$$\mathrm{d^a}(F) = \sup\left\{ \sum_{i\in[n]} u_i \colon c_{\underline{u}} \neq 0 \right\}.$$

For any $x \in \mathbb{F}_p^n$, we can write

$$F(x) = (f_1(x), \ldots, f_m(x))$$

where $f_i\colon \mathbb{F}_p^n \to \mathbb{F}_p$. Then we have that $\mathrm{d^a}(F) = \sup_{j\in[m]} \mathrm{d^a}(f_j)$.

2.3 The binomial coefficient and Integer-Valued (IV) polynomials

Let $n, k \in \mathbb{Z}$, then the binomial coefficient is defined by

$$\binom{n}{k} = \begin{cases} \frac{n(n-1)\cdots(n-k+1)}{k!} & \text{if } k > 0, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0. \end{cases}$$

A known formula is the following. For any $n, k \in \mathbb{Z}$, we have that

$$\binom{n}{k} = (-1)^k \binom{-n+k-1}{k}. \tag{2}$$

Remark 1. We recall that $\binom{n}{k} \in \mathbb{Z}$ for all $n, k \in \mathbb{Z}$. Assume without loss of generality that k is positive. For $n \geq k$, this is known because it refers to the classical binomial coefficient and its connection with the Pascal-Tartaglia triangle. For $0 \leq k \leq n-1$ we have that $\binom{n}{k} = 0$ by definition. If k is negative, then we have $\binom{n}{k} = (-1)^k \binom{-n+k-1}{k}$ and $-n+k-1$ is positive.

Let $p \in \mathbb{N}$ be a prime, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \{0, \ldots, p-1\}$, and $a = \sum_{i \in [n]} a_i p^{i-1}$, $b = \sum_{i \in [n]} b_i p^{i-1}$. We have that the Lucas' Theorem holds:

$$\binom{a}{b} = \prod_{i \in [n]} \binom{a_i}{b_i} \pmod{p}.$$

For us, an *Integer-Valued (IV) polynomial* is any polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ such that when it is evaluated over $\mathbb{Z}^n$ takes values over $\mathbb{Z}$. We will use [CC97] as a reference.

Definition 1. An univariate Integer-Valued (IV) monomial of degree $d \in \mathbb{N}$ is the polynomial $\binom{x}{d}$ in $\mathbb{Q}[x]$.

A multivariate Integer-Valued (IV) monomial of multidegree $(d_1, \ldots, d_n) \in \mathbb{N}^n$ is the polynomial

$$\binom{x_1, \ldots, x_n}{d_1, \ldots, d_n} = \prod_{j=1}^{n} \binom{x_j}{d_j}$$

in $\mathbb{Q}[x_1, \ldots, x_n]$.

An Integer-Valued (IV) polynomial P is a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ that can be written as

$$P(x_1, \ldots, x_n) = \sum_{\underline{d} \in \mathbb{N}^n} P_{\underline{d}} \binom{x_1, \ldots, x_n}{d_1, \ldots, d_n}$$

where $P_{\underline{d}} \in \mathbb{Z}$ and $P_{\underline{d}} \neq 0$ only for finitely many $\underline{d} \in \mathbb{N}^n$.

Proposition 1 ([CC97])**.** *Let $P \colon \mathbb{Z}^n \to \mathbb{Z}$ be induced by an IV polynomial. Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Then we have that*

$$P(x) = \sum_{\underline{d} \in \mathbb{N}^n} \partial^{(\underline{d})} P(0) \binom{x_1, \ldots, x_n}{d_1, \ldots, d_n}. \tag{3}$$

Moreover, for any $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n$ we have that

$$\partial^{(\underline{d})} P(x) = \sum_{\underline{a} \in \mathbb{N}^n \colon a_i \leq d_i} (-1)^{\sum_{i \in [n]} (d_i - a_i)} \binom{d_1, \ldots, d_n}{a_1, \ldots, a_n} P(x + a). \tag{4}$$

3 Threshold Implementations over Abelian groups

The definition of a *Threshold Implementation (TI)* has been generalized in the work by Dhooghe et al. in [DNR19] (section 6) after proving that the threshold implementation technique with *Boolean sharing* (also called *Boolean masking*) is secure in the first-order robust probing secure [DNR19, Theorem 3.2]. We are interested in the case where the secret sharing scheme of both input and output is the *additive sharing* (also called *additive masking*). Let $\mathbb{X}$ be an Abelian group. An *additive s-sharing* of $x \in \mathbb{X}$ is a vector $\underline{x} = (x_1, \ldots, x_s) \in \mathbb{X}^s$ such that $\sum_{i\in[s]} x_i = x$. The set of such vectors is denoted by $\mathrm{Sh}_s(x)$. Notice that $\mathrm{Sh}_s(x) = \underline{x} + \mathrm{Sh}_s(0)$ for all $\underline{x} \in \mathrm{Sh}_s(x)$ and that $\mathrm{Sh}_s(0)$ is an Abelian group of cardinality $|\mathbb{X}|^{s-1}$. Indeed, for any $\underline{x}, \underline{x}' \in \mathrm{Sh}_s(x)$, we have that $\underline{x} - \underline{x}' \in \mathrm{Sh}_s(0)$. In this section, $\mathbb{X}$ and $\mathbb{Y}$ are assumed to be finite Abelian groups.

The correctness property follows from [DNR19, Definition 6.3].

Definition 2 (Correctness)**.** We say that $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ is correct with respect to $F\colon \mathbb{X} \to \mathbb{Y}$ if for any $x \in \mathbb{X}$ and any $\underline{x} \in \mathrm{Sh}_s(x)$ we have that $\mathcal{F}(\underline{x}) \in \mathrm{Sh}_t(F(x))$.

An equivalent definition is that

$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j\in[t]} \mathcal{F}_j(\underline{x})$$

for any $\underline{x} = (x_1, \ldots, x_s) \in \mathbb{X}^s$.

The non-completeness property is almost identical to the one given in [DNR19, Definition 6.4].

Definition 3 (Non-Completeness)**.** We say that $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ is non-complete if for any $j \in [t]$, there exists $i \in [s]$ such that $\partial_a^i \mathcal{F}_j = 0$ for all $a \in \mathbb{X}$.

Indeed, the previous definition implies that any of the output share depends at most on $s-1$ input shares.

Definition 4 (Uniformity)**.** Let $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ be correct with respect to $F\colon \mathbb{X} \to \mathbb{Y}$. We say that $\mathcal{F}$ is uniform if

$$|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}}$$

for any $x \in \mathbb{X}$ and any $\underline{y} \in \mathrm{Sh}_t(F(x))$.

Indeed, the definition given in [DNR19, Definition 6.5] states that there exists a constant $c \in \mathbb{N}$ such that $|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = c$ for any $x \in \mathbb{X}$ and any $\underline{y} \in \mathrm{Sh}_t(F(x))$. This implies that, for any $x \in \mathbb{X}$, the restriction of $\mathcal{F}$ from $\mathrm{Sh}_s(x)$ to $\mathrm{Sh}_t(F(x))$ is balanced, and therefore

$$|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = \frac{|\mathrm{Sh}_s(x)|}{|\mathrm{Sh}_t(F(x))|} = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}}.$$

We are ready to give the definition of threshold implementation.

Definition 5 (Threshold implementation)**.** We say that $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ is a threshold implementation of $F\colon \mathbb{X} \to \mathbb{Y}$ if $\mathcal{F}$ is correct with respect to F, non-complete, and uniform. In this case, we say that F admits a threshold implementation with s shares in input and t shares in output.

As a first theoretical result, we discuss the uniformity property of $\mathcal{F}$ for the cases of F balanced and F bijective.

Proposition 2. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups. Let $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ be correct with respect to $F\colon \mathbb{X} \to \mathbb{Y}$. Then we have the following:*

1. *If $\mathcal{F}$ is uniform, then F is balanced if and only if $\mathcal{F}$ is balanced.*

2. *If F is bijective, then $\mathcal{F}$ is uniform if and only if $\mathcal{F}$ is balanced.*

Proof. Let us prove 1. Let $y \in \mathbb{Y}$ and $\underline{y} \in \mathrm{Sh}_t(y)$. Since $\mathcal{F}$ is uniform, we have that

$$|\mathcal{F}^{-1}(\underline{y})| = \sum_{x \in \mathbb{X}:\ F(x)=y} |\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = |F^{-1}(y)| \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}}.$$

If F is balanced, then $|\mathcal{F}^{-1}(\underline{y})| = \frac{|\mathbb{X}|^s}{|\mathbb{Y}|^t}$ and so $\mathcal{F}$ is balanced. If $\mathcal{F}$ is balanced, then $|F^{-1}(y)| = \frac{|\mathbb{X}|}{|\mathbb{Y}|}$ and so F is balanced.

Let us prove 2. Since F is bijective, then $|\mathbb{X}| = |\mathbb{Y}| = q$. Since any bijective function is balanced, we can use 1 to conclude that if $\mathcal{F}$ is uniform, then $\mathcal{F}$ is balanced. Suppose that $\mathcal{F}$ is balanced and we claim that $\mathcal{F}$ is uniform. Let $\underline{y} = (y_1, \dots, y_t) \in \mathbb{Y}^t$, $y = \sum_{j \in [t]} y_j$, and $x = F^{-1}(y)$. Observe that

$$\left|\mathcal{F}^{-1}(\underline{y})\right| = \sum_{z \in \mathbb{X}:\ F(z)=y} |\mathrm{Sh}_s(z) \cap \mathcal{F}^{-1}(\underline{y})| = \left|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})\right|.$$

Since $\mathcal{F}$ is balanced, then $|\mathcal{F}^{-1}(\underline{y})| = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}} = q^{s-t}$ and $|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = q^{s-t}$. This concludes the proof. □

Remark 2. According to Proposition 2, we have that $\mathcal{F}$ can be both uniform and unbalanced if F is also unbalanced. We show an example of this case. Let $F\colon \mathbb{Z}_4 \to \mathbb{Z}_2$ defined by $F(0) = 0$, $F(1) = 0$, $F(2) = 0$, and $F(3) = 1$. Let $\mathcal{F}\colon \mathbb{Z}_4^2 \to \mathbb{Z}_2^2$ be defined as follow:

$$\begin{aligned}
&\mathcal{F}(\underline{x}) = (0,0),\ \underline{x} \in \{(0,0),(0,1),(0,2),(1,3),(1,0),(1,1)\},\\
&\mathcal{F}(\underline{x}) = (1,1),\ \underline{x} \in \{(2,2),(2,3),(2,0),(3,1),(3,2),(3,3)\},\\
&\mathcal{F}(\underline{x}) = (1,0),\ \underline{x} \in \{(0,3),(1,2)\},\\
&\mathcal{F}(\underline{x}) = (0,1),\ \underline{x} \in \{(2,1),(3,0)\}.
\end{aligned}$$

By construction, we have that $\mathcal{F}$ is unbalanced and it is correct with respect to F. One can verify that $|\mathrm{Sh}_2(x) \cap \mathcal{F}^{-1}(\underline{y})| = 2 = \frac{|\mathbb{Z}_4|^{2-1}}{|\mathbb{Z}_2|^{2-1}}$ for all $x \in \mathbb{Z}_2$ and all $\underline{y} \in \mathrm{Sh}_2(F(x))$. So we have that $\mathcal{F}$ is uniform.

Remark 3. According to Proposition 2, we have that if F is bijective then the uniform property of $\mathcal{F}$ coincides with balancedness property. If F is balanced, then we can only say that the uniformity property implies balancedness but not the other implication. For instance, consider the balanced function $F\colon \mathbb{Z}_4 \to \mathbb{Z}_2$ defined by $F(0) = 0$, $F(1) = 0$, $F(2) = 1$, and $F(3) = 1$. Let $\mathcal{F}\colon \mathbb{Z}_4^2 \to \mathbb{Z}_2^2$ be defined as follow:

$$\begin{aligned}
&\mathcal{F}(\underline{x}) = (0,0),\ \underline{x} \in \{(0,0),(1,0),(2,3),(3,2)\},\\
&\mathcal{F}(\underline{x}) = (1,1),\ \underline{x} \in \{(0,1),(1,3),(2,2),(3,1)\},\\
&\mathcal{F}(\underline{x}) = (1,0),\ \underline{x} \in \{(0,2),(1,2),(2,1),(3,0)\},\\
&\mathcal{F}(\underline{x}) = (0,1),\ \underline{x} \in \{(0,3),(1,1),(2,0),(3,3)\}.
\end{aligned}$$

By construction, we have that $\mathcal{F}$ is correct with respect to F and $\mathcal{F}$ is balanced. However, $\mathcal{F}$ is not uniform because $|\mathrm{Sh}_2(0) \cap \mathcal{F}^{-1}(0,0)| = 1 \neq \frac{|\mathbb{Z}_4|^{2-1}}{|\mathbb{Z}_2|^{2-1}} = 2$.

3.1 A note on Inner Product Masking

The Inner Product Masking (IPM) [BFG15] is a kind of masking (or sharing) over $\mathbb{F}_{2^n}$ where the vector of shares $\underline{x} = (x_1, \ldots, x_s) \in (\mathbb{F}_{2^n})^s$ of $x \in \mathbb{F}_{2^n}$ is such that $x = \sum_{i\in[s]} c_i x_i$ for some fixed $c_i \in \mathbb{F}_{2^n} \setminus \{0\}$. Such sharing is easy to generalize by keeping desirable properties.

Let $\mathcal{S}\colon \mathbb{X}^s \to \mathbb{X}^s$ be such that, for any $i \in [s]$, $\mathcal{S}_i(\underline{x}) = S_i(x_i)$ where S_i is a permutation of $\mathbb{X}$ (a special case is $S_i(x) = c_i x$ for IPM). For this sharing, the vector of shares $\underline{x} = (x_1, \ldots, x_s) \in \mathbb{X}^s$ of $x \in \mathbb{X}$ is such that $x = \sum_{i\in[s]} S_i(x_i)$. Let us denote $\mathrm{Sh}_s^{\mathcal{S}}(x)$ the set of such vectors of shares. We still have that $|\mathrm{Sh}_s^{\mathcal{S}}(x)| = |\mathbb{X}|^{s-1}$ because $\mathrm{Sh}_s^{\mathcal{S}}(x) = \mathcal{S}(\mathrm{Sh}_s(x))$ and $\mathcal{S}$ is a bijection. Moreover, if $\mathcal{S}$ is linear then $\mathrm{Sh}_s^{\mathcal{S}}(0)$ is an Abelian group and $\mathrm{Sh}_s^{\mathcal{S}}(x)$ is one of its coset. Let $\mathcal{T}\colon \mathbb{Y}^t \to \mathbb{Y}^t$ be such that, for any $j \in [t]$, $\mathcal{T}_j(\underline{y}) = T_j(y_i)$ where T_j is a permutation of $\mathbb{Y}$. Let $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ and $\mathcal{F}'\colon : \mathbb{X}^s \to \mathbb{Y}^t$ defined by $\mathcal{F}' = \mathcal{T}^{-1} \circ \mathcal{F} \circ \mathcal{S}$. We claim that if $\mathcal{F}$ has one of the property between correctness, non-completeness, and uniformity then $\mathcal{F}'$ has the same property with respect to the IPM (defined by in [DNR19]).

If $\mathcal{F}$ is non-complete then also $\mathcal{F}'$ is non-complete because, for any $j \in [t]$ and any $x_1, \ldots, x_s \in \mathbb{X}$, we have that

$$\mathcal{F}'_j(x_1, \ldots, x_s) = T_j^{-1}\left(\mathcal{F}_j(S_1(x_1), \ldots, S_s(x_s))\right).$$

If $\mathcal{F}$ is correct with respect to a function $F\colon \mathbb{X} \to \mathbb{Y}$ then for any $x_1, \ldots, x_s \in \mathbb{X}$ we have

$$\begin{aligned} F\left(\sum_{i\in[s]} S_i(x_i)\right) &= \sum_{j\in[t]} \mathcal{F}_j(S_1(x_1), \ldots, S_s(x_s)) \\ = \sum_{j\in[t]} T_j\left(T_j^{-1}\left(\mathcal{F}_j(\mathcal{S}(\underline{x}))\right)\right) &= \sum_{j\in[t]} \mathcal{F}'_j(\underline{x}). \end{aligned}$$

If $\mathcal{F}$ is uniform then, for any $x \in \mathbb{X}$, the restriction $\mathcal{F}'\colon \mathrm{Sh}_s^{\mathcal{S}}(x) \to \mathrm{Sh}_t^{\mathcal{T}}(F(x))$ is balanced since it is obtained by composing the bijection $\mathcal{S}\colon \mathrm{Sh}_s^{\mathcal{S}}(x) \to \mathrm{Sh}_s(x)$, the balanced function $\mathcal{F}\colon \mathrm{Sh}_s(x) \to \mathrm{Sh}_t(F(x))$, and the bijection $\mathcal{T}\colon \mathrm{Sh}_t(F(x)) \to \mathrm{Sh}_t^{\mathcal{T}}(F(x))$.

4 Functional degree, functional expansions, and non-completeness

Let $F\colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups. Let s be a positive integer. We say that F admits a *functional expansion of the s-th order* if there exists a family of integers $\{k_I\}_{I\in\mathcal{P}_{s,j},\, j<s}$ such that

$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j=0}^{s-1} \sum_{I\in\mathcal{P}_{s,j}} k_I \cdot F\left(\sum_{i\in I} x_i\right)$$

for all $x_1, \ldots, x_s \in \mathbb{X}$. In [CPRR15, Corollary 1], it was shown that every function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ admits a functional expansion of the s-th order where $s \geq \mathrm{d}^{\mathrm{a}}(F) + 1$. Moreover, we have that if $\mathcal{F}\colon (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^t$ is non-complete and correct with respect to F, then both s and t must be greater or equal than $\mathrm{d}^{\mathrm{a}}(F)+1$ [NRR06, Theorem 1]. Indeed, one can use a functional expansion of the s-th order and construct $\mathcal{F}$. This observation was made first in [PAB+23] and used to construct a family of threshold implementations. So clearly there is a connection between functional expansions and the algebraic degree of F. In this section, we want to achieve similar results for a notion of degree that can be defined for any $F\colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups and by using the definitions introduced in Section 3. We will show that such notion is the one of *functional degree*

introduced by Aichinger and Moosbauer in [AM21]. Most of the time, we are not going to restrict ourselves to the cases of $\mathbb{X}$ and $\mathbb{Y}$ to be finite because we will need some results for Section 6. Moreover, observe that also the definitions of correctness and non-completeness do not need $\mathbb{X}$ and $\mathbb{Y}$ to be finite.

Instead of using the definition of functional degree given in [AM21, Definition 2.1] which is in terms of abstract algebra, we will use the equivalent one given in terms of Fréchet's equation

$$\Delta_{\underline{a}}^{(d+1)} F = 0. \tag{5}$$

Definition 6 (Functional degree)**.** Let $F\colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups. We denote the functional degree of F as

$$\mathrm{d}^\circ(F) = \inf\{d \in \mathbb{N} \mid \Delta_{\underline{a}}^{(d+1)} F = 0, \text{ for all } \underline{a} \in \mathbb{X}^{d+1}\}.$$

Aichinger and Moosbauer in [AM21] do not mention the fact that this notion of degree is strictly related with the theory of Integer-Valued polynomials. Indeed, this was first observed by a previous work [Sch14] and then the connection was clarified in [CS22]. We will present this in Section 6 since we do not need it for now.

Some of the properties the functional degree satisfies are the following:

- $\mathrm{d}^\circ(F) = 0$ if and only if F is constant [AM21, Lemma 3.1].
- $\mathrm{d}^\circ(F) \leq 1$ if and only if F is affine [AM21, Lemma 3.1].
- If $0 < \mathrm{d}^\circ(F) < \infty$, then $\mathrm{d}^\circ(\Delta_a F) < \mathrm{d}^\circ(F)$ for all $a \in \mathbb{X}$ [AM21, Lemma 3.1].
- $\mathrm{d}^\circ(F+G) \leq \sup\{\mathrm{d}^\circ(F), \mathrm{d}^\circ(G)\}$ and $\mathrm{d}^\circ(F+G) = \mathrm{d}^\circ(F)$ if $\mathrm{d}^\circ(F) > \mathrm{d}^\circ(G)$ [AM21, Lemma 3.2].
- If $\mathrm{d}^\circ(F) < \infty$ and $\mathrm{d}^\circ(G) < \infty$, then $\mathrm{d}^\circ(F \circ G) \leq \mathrm{d}^\circ(F) \cdot \mathrm{d}^\circ(G)$ [AM21, Theorem 4.3].
- If $\mathbb{Y}$ is a ring, then $\mathrm{d}^\circ(F \cdot G) \leq \mathrm{d}^\circ(F) + \mathrm{d}^\circ(G)$ [AM21, Lemma 6.1].

By using [AM21, Theorem 10.3], it is straightforward to prove that the notion of functional degree coincides with the one of algebraic degree for the case of functions between finite-dimensional vector spaces over $\mathbb{F}_p$ where p is a prime. For completeness, we give a short proof of this result.

Lemma 1 ([AM21, Lemma 3.4])**.** *Let $F\colon \mathbb{X} \to \prod_{j\in[m]} \mathbb{Y}_j$ where $\mathbb{X}, \mathbb{Y}_1, \ldots, \mathbb{Y}_m$ are Abelian groups. Let $F = (F_1, \ldots, F_m)$ where $F_j\colon \mathbb{X} \to \mathbb{Y}_j$ for any $j \in [m]$. Then we have that*

$$\mathrm{d}^\circ(F) = \sup_{j\in[m]} \mathrm{d}^\circ(F_j).$$

Proposition 3. *Let p be a prime and let $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$. Then $\mathrm{d}^\circ(F) = \mathrm{d}^{\mathrm{a}}(F)$.*

Proof. Let $F = (f_1, \ldots, f_m)$ where $f_j\colon \mathbb{F}_p^n \to \mathbb{F}_p$ for $j \in [m]$. Then $\mathrm{d}^{\mathrm{a}}(F) = \sup_{j\in[m]} \mathrm{d}^{\mathrm{a}}(f_j)$. Let $j \in [m]$. Then $d_j = \mathrm{d}^{\mathrm{a}}(f_j)$ is exactly the degree of the multivariate polynomial in (1). To conclude the proof, observe that we have that $\mathrm{d}^\circ(f_j) = d_j = \mathrm{d}^{\mathrm{a}}(f_j)$ by [AM21, Theorem 10.3] and that $\mathrm{d}^\circ(F) = \sup_{j\in[m]} \mathrm{d}^\circ(f_j)$ by Lemma 1. □

4.1 Functional expansions and non-completeness

In [AM21, Lemma 4.1], it is proven that for a function F to have finite functional degree is equivalent to three other properties. By using the definitions introduced in this paper, the first two can be described as the existence of particular functional expansions of F while the last one is the existence of a specific function $\mathcal{F}$ which is correct with respect to F and non-complete. We present the following lemma in our notation and prove that is equivalent to [AM21, Lemma 4.1].

Lemma 2. *Let d be a positive integer. Let $F\colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups. Then the following are equivalent:*

1. $\mathrm{d}^\circ(F) \leq d$.
2. *For every positive integer $s \geq d+1$, the function F admits the following functional expansion of the s-th order:*
$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j=0}^{s-1}(-1)^{s-1-j} \sum_{I\in\mathcal{P}_{s,j}} F\left(\sum_{i\in I} x_i\right).$$
3. *For every positive integer $s \geq d+1$, the function F admits a functional expansion of the s-th order for some family of integers $\mathcal{K}_s = \{k_I\}_{I\in\mathcal{P}_{s,j},\, j<s}$ where $k_I = 0$ for all $I \in \mathcal{P}_{s,j}$ with $j \geq d+1$.*
4. *For every positive integer $s \geq d+1$, there exists a function $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^{d+1}$ which is correct with respect to F and non-complete.*

Proof. 1, 2, 3 are equivalent respectively to the first three items in [AM21, Lemma 4.1]. Let us call 4a the fourth item in [AM21, Lemma 4.1] which states that there exists functions $\mathcal{F}_1, \ldots, \mathcal{F}_{d+1}\colon \mathbb{X}^{d+1} \to \mathbb{Y}$ such that for all $\underline{x} = (x_1, \ldots, x_{d+1}) \in \mathbb{X}^{d+1}$ we have $F\left(\sum_{i\in[d+1]} x_i\right) = \sum_{j\in[d+1]} \mathcal{F}_j(\underline{x})$ and for each $j \in [d+1]$, the function $\mathcal{F}_j$ does not depend on its j-th coordinate. We show that 4 is equivalent to 4a. It is clear that 4a implies 4 since for any $s \geq d+1$, we can set $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{d+1}, 0, \ldots, 0)$. We conclude by proving that 4 implies 4a. Let $\mathcal{F}\colon \mathbb{X}^{d+1} \to \mathbb{Y}^{d+1}$ be correct with respect to F and non-complete. Let $\mathcal{F}_1, \ldots, \mathcal{F}_{d+1}\colon \mathbb{X}^{d+1} \to \mathbb{Y}$ be such that $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{d+1})$. We define $J_1 = \{i \in [d+1] \mid \partial_a^1 \mathcal{F}_i = 0 \text{ for all } a \in \mathbb{X}\}$ and $J_j = \{i \in [d+1] \setminus J_{j-1} \mid \partial_a^j \mathcal{F}_i = 0 \text{ for all } a \in \mathbb{X}\}$ for $j \in [2, d+1]$. Set $\mathcal{F}'_j = \sum_{i\in J_j} \mathcal{F}_i$ where we recall that $\sum_{i\in\emptyset} \mathcal{F}_i = 0$. Then $\mathcal{F}'_1, \ldots, \mathcal{F}'_{d+1}$ satisfies 4a. □

With the following proposition, we generalize [NRR06, Theorem 1] for our setting.

Proposition 4. *Let d be a positive integer. Let $F\colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups. Let $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ be correct with respect to F. If $\mathrm{d}^\circ(F) = d$ and $\mathcal{F}$ is non-complete, then s and t are greater or equal than $d+1$.*

Proof. Suppose that $t \leq d$. Let $\underline{x} = (x_1, \ldots, x_s) \in \mathbb{X}^s$. Since $\mathcal{F}$ is non-complete, then for any $j \in [t]$ there exists $i_j \in [s]$ such that $\partial_a^{i_j} \mathcal{F}_j(\underline{x}) = 0$ for all $a \in \mathbb{X}$. Let $\mathcal{H}(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right)$, $x = \sum_{i\in[s]} x_i$, and $\underline{a} = (a_1, \ldots, a_t) \in \mathbb{X}^t$. Then we have that

$$0 = \sum_{j\in[t]} \partial_{a_j}^{i_j} \mathcal{F}_j(\underline{x}) = \partial_{a_1}^{i_1} \cdots \partial_{a_t}^{i_t} \sum_{j\in[t]} \mathcal{F}_j(\underline{x}) = \partial_{a_1}^{i_1} \cdots \partial_{a_t}^{i_t} \mathcal{H}(\underline{x}) = \Delta_{\underline{a}}^{(t)} F(x)$$

because

$$\partial_a^k \mathcal{H}(\underline{x}) = F\left(\sum_{i\in[s]} x_i + a\right) - F\left(\sum_{i\in[s]} x_i\right) = \Delta_a F(x)$$

for any $k \in [s]$ and any $a \in \mathbb{X}$. Therefore, we have that $\Delta_{\underline{a}}^{(t)} F(x) = 0$ but this is not possible because $\mathrm{d}^\circ(F) = d > t - 1$. So we have that $t \geq d + 1$. Suppose that $s \leq d$ and $t \geq d + 1$. By item 4 of Lemma 2, this implies that $\mathrm{d}^\circ(F) = d < s$ and this is not possible since $s \leq d$. □

Lemma 2 and Proposition 4 are the evidence that the functional degree is a suitable notion of degree for the threshold implementation theory with additive sharing.

A natural problem that rises from Lemma 2 is to give an explicit form of the functional expansion described in item 3. To the best of our knowledge, we are not aware if this result is known for the general case. In the binary case, this problem was solved in [CPRR15, Corollary 1].

Proposition 5. *Let d be a positive integer. Let $\mathbb{X}$ and $\mathbb{Y}$ be Abelian groups and $F \colon \mathbb{X} \to \mathbb{Y}$. Then $\mathrm{d}^\circ(F) \leq d$ if and only if for any positive integer $s \geq d + 1$, F admits the following functional expansion of the s-th order:*

$$F\left(\sum_{i \in [s]} x_i\right) = \sum_{j=0}^{d} \mu_{s,d}(j) \sum_{I \in \mathcal{P}_{s,j}} F\left(\sum_{i \in I} x_i\right) \tag{6}$$

where $\mu_{s,d}(j) = \binom{s-j-1}{d-j}(-1)^{d-j}$.

Proof. The proof is in Appendix A.1. □

4.2 On the case where the domain and the codomain are finite

In [AM21], they describe all the functions $F \colon \mathbb{X} \to \mathbb{Y}$ with finite functional degree where $\mathbb{X}$ and $\mathbb{Y}$ are finite Abelian groups. For completeness, we present also the following lemma.

Lemma 3 ([AM21, Lemma 7.1 and Lemma 9.3])**.** *Let p, q be prime numbers and let $n, m \in \mathbb{N}$. Let $\mathbb{X}$ and $\mathbb{Y}$ be Abelian groups such that $|\mathbb{X}| = p^n$ and $|\mathbb{Y}| = q^m$. Let $F \colon \mathbb{X} \to \mathbb{Y}$. Then $\mathrm{d}^\circ(F) < \infty$ if and only if either $p = q$, $n = 0$, or $m = 0$.*

Proposition 6 ([AM21, Theorem 9.4])**.** *Let $p_1, \ldots, p_n$ be distinct primes. For any $i \in [n]$, let $\mathbb{X}_i$ and $\mathbb{Y}_i$ be Abelian groups such that $|\mathbb{X}_i| = p_i^{m_i}$ and $|\mathbb{Y}_i| = p_i^{k_i}$ for some $m_i, k_i \in \mathbb{N}$. Let $\mathbb{X} = \prod_{i \in [n]} \mathbb{X}_i$, $\mathbb{Y} = \prod_{i \in [n]} \mathbb{Y}_i$, and let $F \colon \mathbb{X} \to \mathbb{Y}$. Write $F = (F_1, \ldots, F_n)$ where $F_j \colon \mathbb{X} \to \mathbb{Y}_j$ for any $j \in [n]$. Then $\mathrm{d}^\circ(F) < \infty$ if and only if for all $i, j \in [n]$ such that $i \neq j$ we have that $\partial_a^i F_j = 0$ for all $a \in \mathbb{X}_i$.*

Remark 4. Observe that for any finite Abelian groups $\mathbb{X}$ and $\mathbb{Y}$ we can find a decomposition as in Proposition 6. Indeed, let $p_1, \ldots, p_n$ be all the distinct primes that divides the positive integer $|\mathbb{X}| \cdot |\mathbb{Y}|$. Then we can write $\mathbb{X} = \prod_{i \in [n]} \mathbb{X}_i$ and $\mathbb{Y} = \prod_{i \in [n]} \mathbb{Y}_i$ where for any $i \in [n]$, $\mathbb{X}_i$ and $\mathbb{Y}_i$ are Abelian groups of order a power of p_i. Let $F \colon \mathbb{X} \to \mathbb{Y}$. If F has finite functional degree, then there exist functions $F_i \colon \mathbb{X}_i \to \mathbb{Y}_i$ for any $i \in [n]$ such that

$$F(x_1, \ldots, x_n) = (F_1(x_1), \ldots, F_n(x_n))$$

for all $(x_1, \ldots, x_n) \in \mathbb{X} = \prod_{i \in [n]} \mathbb{X}_i$.

5 On the construction of threshold implementations with $d + 2$ shares

In this section, we are going to generalize the construction defined in [PAB+23]. We will consider those functions $F \colon \mathbb{X} \to \mathbb{Y}$ between two finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$ and $\mathrm{d}^\circ(F) < \infty$. The hypothesis $\mathrm{d}^\circ(F) < \infty$ is strictly necessary because

of Lemma 2. We impose that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$ because we will need the existence of at least one balanced function $P\colon \mathbb{X} \to \mathbb{Y}$. First, we give a general theorem that serves as a tool to construct functions $\mathcal{F}$ that are correct and uniform. Then we present a functional expansion into terms that can be distributed in the coordinate functions of $\mathcal{F}$ in order to make it non-complete.

To give a proper generalization of the construction in [PAB+23], we need to consider the following subclass of the class of balanced functions.

Definition 7 (Balanced affine fibers)**.** Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups. We say that $F\colon \mathbb{X} \to \mathbb{Y}$ has balanced affine fibers if there exists a subgroup $\mathbb{X}'$ of $\mathbb{X}$ such that $F^{-1}(y)$ is a coset of $\mathbb{X}'$ for all $y \in \mathbb{Y}$.

In Definition 7, we are using the term "affine" improperly since those fibers are actually cosets of a subgroup. However, if $\mathbb{X} = \mathbb{F}_p^n$ then every subgroup is a vector space over $\mathbb{F}_p$ and its cosets are indeed affine spaces.

Remark 5. Observe that if F has balanced affine fibers then, for any $y, y' \in \mathbb{Y}$ with $y \neq y'$, we have that $F^{-1}(y_1)$ and $F^{-1}(y_2)$ are two different cosets of $\mathbb{X}'$. So we have that $|\mathbb{Y}| = |\mathbb{X}|/|\mathbb{X}'|$ and that F is balanced. Moreover, there always exists a subgroup $\mathbb{X}'$ of $\mathbb{X}$ of order $|\mathbb{X}|/|\mathbb{Y}|$. So the existence of at least one function with balanced affine fibers is always guaranteed by the condition "$|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$". An example of functions that have affine fibers are surjective affine functions, but those exists only if $\mathbb{Y}$ is isomorphic to a subgroup of $\mathbb{X}$. Moreover, for the case $|\mathbb{X}| = |\mathbb{Y}|$ we have that the notion of having balanced affine fibers coincides with the notion of being bijective.

In the following, we have the main theorem of this section that provides a general form for the construction of a correct and uniform function.

Theorem 1. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. Let $F\colon \mathbb{X} \to \mathbb{Y}$ be any function. Let s and t be positive integers such that $2 \leq t \leq s$. For any $j \in \{1, \ldots, t-1\}$, let $P_j\colon \mathbb{X} \to \mathbb{Y}$ be balanced and let $\mathcal{C}_j\colon \mathbb{X}^j \to \mathbb{Y}$. Let $\underline{b} = (b_1, \ldots, b_{t-1}) \in \{0,1\}^{t-1}$ and let $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ be a function defined as follow for any $\underline{x} = (x_1, \ldots, x_s) \in \mathbb{X}^s$:*

$$\mathcal{F}_t(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right) - \sum_{j\in[t-1]} \mathcal{F}_j(\underline{x})$$

and for any $j \in [t-1]$ we have

$$\mathcal{F}_j(\underline{x}) = (1-b_j)\cdot P_j\left(x_j\right) + b_j \cdot P_j\left(\sum_{i\in[j+1,s]} x_i\right) + \mathcal{C}_j(\underline{x}^{(j)}),$$

where $\underline{x}^{(j)} = ((x_i)_{i\in[j-1]}, \sum_{i\in[j,s]} x_i)$ with the abuse of notation that $\underline{x}^{(1)} = \sum_{i\in[s]} x_i$.
Then the following holds:

1. *$\mathcal{F}$ is correct with respect to F.*
2. *If for each $j \in [t-1]$ with $b_j = 1$ the function P_j has balanced affine fibers, then $\mathcal{F}$ is uniform.*

Proof. Let us prove 1. Function $\mathcal{F}$ is correct with respect to F because

$$\sum_{j\in[t]} \mathcal{F}_j(\underline{x}) = \sum_{j\in[t-1]} \mathcal{F}_j(\underline{x}) + \mathcal{F}_t(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right).$$

Let us prove 2. Let $x \in \mathbb{X}$ and let $\underline{y} \in \mathrm{Sh}_t(F(x))$. Consider the system

$$\begin{cases} y_1 = \mathcal{F}_1(\underline{x}) \\ y_2 = \mathcal{F}_2(\underline{x}) \\ \dots \\ y_t = \mathcal{F}_t(\underline{x}) \\ x = \sum_{i\in[s]} x_i \end{cases} \tag{7}$$

in the variable $\underline{x} \in \mathbb{X}^s$. Observe that the number of solutions of system (7) is equal to $|\mathrm{Sh}_s(x) \cap (\mathcal{F})^{-1}(\underline{y})|$. So if we prove that system (7) has exactly $|\mathbb{X}|^{s-1}/|\mathbb{Y}|^{t-1}$ solutions, then we have that $\mathcal{F}$ is uniform. To do that, we are going to turn system (7) into a triangular system. Observe that by summing the first t equations of system (7), we have that $\sum_{j\in[t]} y_j = \sum_{j\in[t]} \mathcal{F}_j(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right) = F(x)$. So we can replace the t-th equation of system (7) with the equation $\sum_{j\in[t]} y_j = F(x)$. For any $j \in [t-1]$, we claim that we can replace the j-th equation of system (7) with a condition of the form $x_j \in \Gamma_j(x_i)_{i\in[j-1]}$ where $\Gamma_j(x_i)_{i\in[j-1]} \subseteq \mathbb{X}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$ for all $(x_i)_{i\in[j-1]} \in \mathbb{X}^{j-1}$. So we have that system (7) is equivalent to the following system

$$\begin{cases} x_j \in \Gamma_j(x_i)_{i\in[j-1]}, \quad j \in [t-1] \\ \sum_{j\in[t]} y_j = F(x) \\ x = \sum_{i\in[s]} x_i \end{cases} . \tag{8}$$

System (8) can be solved in the following way. Let $\underline{x} \in \mathbb{X}^s$ be any solution of system (8). By solving the first $t-1$ equations in order, we have that the number of choices of the first $t-1$ coordinates of $\underline{x}$ are exactly $(|\mathbb{X}|/|\mathbb{Y}|)^{t-1}$. Observe that the t-th equation is not written in term of $\underline{x}$. By using the $t+1$-th equation, we have that there are $|\mathbb{X}|^{s-t}$ choices for the the remaining $s-t$ coordinates of $\underline{x}$. So the number of solutions of system (8) is $(|\mathbb{X}|)^{s-1}/(|\mathbb{Y}|)^{t-1}$ and so is the number of solution of system (7).

Let us prove that for any $j \in [t-1]$ we can replace the j-th equation of system (7) with a condition of the form $x_j \in \Gamma_j(x_i)_{i\in[j-1]}$ where $\Gamma_j(x_i)_{i\in[j-1]} \subseteq \mathbb{X}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$. By using the $t+1$-th equation of system (7), we have that $\sum_{i\in[j,s]} x_i = x - \sum_{i\in[j-1]} x_i$. Therefore, the term $\mathcal{C}_j(\underline{x}^{(j)})$ depends only on $(x_i)_{i\in[j-1]}$. Suppose that $b_j = 0$. Then $y_j = P_j(x_j) + \mathcal{C}_j(\underline{x}^{(j)})$ and so we have that

$$\Gamma_j(x_i)_{i\in[j-1]} = P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right)$$

and that $\Gamma_j(x_i)_{i\in[j-1]}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$ because P_j is balanced. Suppose that $b_j = 1$, then P_j has balanced affine fibers. Then $y_j = P_j(\sum_{i\in[j+1,s]} x_i) + \mathcal{C}_j(\underline{x}^{(j)})$ and $x_j \in \Gamma_j(x_i)_{i\in[j-1]} = (x - \sum_{i\in[j-1]} x_i) - P_1^{-1}(y_1 - \mathcal{C}_1(x))$ because

$$\begin{aligned} y_j &= P_j\left(\sum_{i\in[j+1,s]} x_i\right) + \mathcal{C}_j(\underline{x}^{(j)}) \\ \sum_{i\in[j+1,s]} x_i &\in P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right) \\ x - x_j - \sum_{i\in[j-1]} x_i &\in P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right) \end{aligned}$$

by using the $t+1$-th equation of system (7). We claim that $\Gamma_j(x_i)_{i\in[j-1]}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$. Since P_j has balanced affine fibers, the set $P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right)$ is a coset of an

Abelian group of cardinality $|\mathbb{X}|/|\mathbb{Y}|$ and so is any of its translation. This proves that $\Gamma_j(x_i)_{i\in[j-1]}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$. □

In the previous theorem, we have established some sufficient condition to construct a correct and uniform function. With the following lemma, we will address the non-completeness property. This follows the same rationale of the proof of the construction in [PAB+23].

Lemma 4. *Let $F\colon \mathbb{X} \to \mathbb{Y}$ be a function such that $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups. If $d = \mathrm{d}^\circ(F) < \infty$, then for any positive integer $s \geq d+2$ we have that F admits the following functional expansion of the s-th order:*

$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j\in[2,d+1]} \sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) + \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right).$$

Proof. Let $z_i = x_i$ for $i = 1,\dots,d$ and $z_{d+1} = \sum_{i\in[d+1,s]} x_i$. Then the result follows by using [PAB+23, Lemma 2] and Lemma 2:

$$\begin{aligned}
F\left(\sum_{i\in[s]} x_i\right) &= F\left(\sum_{i\in[d+1]} z_i\right) = \sum_{I'\in\mathcal{P}^*_{d+1}} (-1)^{d-|I'|} F\left(\sum_{i\in I'} z_i\right) \\
&= \sum_{j\in[2,d+1]} \sum_{I\in\mathcal{P}_{j-2}} (-1)^{d-|I|-(d-j)} F\left(\sum_{i\in I} z_i + \sum_{i\in[j,d+1]} z_i\right) + \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} z_i\right) \\
&= \sum_{j\in[2,d+1]} \sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) + \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right).
\end{aligned}$$

□

Lemma 5. *Suppose to be in the hypothesis of Theorem 1 including the ones of item 2. Let d be a positive integer. If $\mathrm{d}^\circ(F) \leq d$ and $t = d+2$, then there exists at least one choice of $\mathcal{C}_1,\dots,\mathcal{C}_{d+1}$ such that the following holds:*

- *$\mathcal{C}_1$ is constant,*
- *for any $j \in [2, d+1]$ and any $a \in \mathbb{X}$ we have that $\partial_a^{j-1}\mathcal{C}_j = 0$.*
- *there exists $k \in [d+1, s]$ such that $\partial_a^k \mathcal{F}_{d+2} = 0$ for all $a \in \mathbb{X}$.*

In this case, $\mathcal{F}$ is a threshold implementation of F.

Proof. We set $\mathcal{C}_1 = 0$ and

$$\mathcal{C}_j(\underline{x}^{(j)}) = \sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) - b_{j-1}\cdot P_{j-1}\left(\sum_{i\in[j,s]} x_i\right)$$

for any $j \in [2, d+1]$ and any $\underline{x} \in \mathbb{X}^s$. So $\mathcal{C}_1,\dots,\mathcal{C}_{d+1}$ satisfy the first two items. Let us

prove the last item. By using Lemma 4, we have that $\mathcal{F}_{d+2}(\underline{x})$ is equal to

$$\begin{aligned}
&F\left(\sum_{i\in[s]} x_i\right) - \sum_{j\in[d+1]} \left(\mathcal{C}_j(\underline{x}^{(j)}) + (1-b_j)\cdot P_j\left(x_j\right) + b_j \cdot P_j\left(\sum_{i\in[j+1,s]} x_i\right)\right)\\
=&F\left(\sum_{i\in[s]} x_i\right) - \sum_{j\in[2,d+1]} \sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right)\\
&- \sum_{j\in[d+1]} (1-b_j)\cdot P_j\left(x_j\right) - b_{d+1}\cdot P_{d+1}\left(\sum_{i\in[d+2,s]} x_i\right)\\
=&\sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right) - \sum_{j\in[d+1]} (1-b_j)\cdot P_j\left(x_j\right) - b_{d+1}\cdot P_{d+1}\left(\sum_{i\in[d+2,s]} x_i\right).
\end{aligned}$$

So we have that $\partial_a^{d+2}\mathcal{F}_{d+2}(\underline{x}) = 0$ if $b_{d+1} = 0$ and $\partial_a^{d+1}\mathcal{F}_{d+2}(\underline{x}) = 0$ if $b_{d+1} = 1$.

Let us show that $\mathcal{F}$ is a threshold implementation of F. The function $\mathcal{F}$ is correct with respect to F by item 1 of Theorem 1. Since the hypothesis of item 2 of Theorem 1 is satisfied, then $\mathcal{F}$ is uniform. To conclude, we claim that $\mathcal{F}$ is non-complete. Let $a \in \mathbb{X}$ and $\underline{x} \in \mathbb{X}^s$. Since $\mathcal{C}_1$ is constant, we have that $\partial_a^2\mathcal{F}_1 = 0$ if $b_1 = 0$ and $\partial_a^1\mathcal{F}_1 = 0$ if $b_1 = 1$. For any $j \in [2, d+1]$, we have that $\partial_a^{j-1}\mathcal{F}_j = \partial_a^{j-1}\mathcal{C}_j = 0$. Then there exists $k \in [d+1, s]$ such that $\partial_a^k\mathcal{F}_{d+2} = 0$. □

Remark 6. Let $\mathcal{F}$ be as in Lemma 5. If F is has balanced affine fibers (e.g., bijective), we can set $P_j = F$ for all $j \in [t-1]$. If F is balanced and does not have balanced affine fibers, we can still set $b_j = 0$ and $P_j = F$ for all $j \in [t-1]$.

Theorem 2. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. Let s, d be positive integers such that $s \geq d+2$. Then any function $F\colon \mathbb{X} \to \mathbb{Y}$ with functional degree at most d admits a threshold implementation $\mathcal{F}$ with s shares in input and $d+2$ shares in output.*

Proof. Take $\mathcal{F}$ as in Lemma 5. □

Corollary 1. *Let m, n, p, s, d be positive integers such that $m \leq n$, $s \geq d+2$, and p is a prime. Then any function $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ with algebraic degree at most d admits a threshold implementation $\mathcal{F}$ with s shares in input and $d+2$ shares in output.*

Proof. By Proposition 3, we have that $\mathrm{d}^\circ(F) = \mathrm{d}^{\mathrm{a}}(F)$. So we can conclude by Theorem 2. □

Remark 7 (On the curious case where $\mathbb{X}$ and $\mathbb{Y}$ are not finite). Let $F\colon \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups not necessarily finite. In this case, the correctness property and the non-completeness property are still well-defined while the uniformity property needs the notion of balancedness which is not well defined if $\mathbb{X}$ or $\mathbb{Y}$ have infinite cardinality. However, there is a special case in which we can still give a notion of uniformity that is the case where $|\mathbb{X}| = |\mathbb{Y}|$ and $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^s$. We can say that $\mathcal{F}$ is uniform if and only if for any $x \in \mathbb{X}$ the restriction of $\mathcal{F}\colon \mathrm{Sh}_s(x) \to \mathrm{Sh}_s(F(x))$ is bijective. So it is straightforward to adapt Theorem 1 by using the term "bijective" everywhere we have the term "balanced". Moreover, we recall that Lemma 4 do not require $\mathbb{X}$ and $\mathbb{Y}$ to be finite. Since this generalization is out of the scope of this paper, we will not provide a proof of this claim.

5.1 The multiplication map

We provide an example on how to construct a threshold implementation with 4 shares for the multiplication map.

Let R be a finite ring. Let $F\colon R^2 \to R$ be the multiplication map, i.e. $F(a,b) = ab$. Then F has functional degree 2. Indeed, it is not affine so we have that $\mathrm{d}^\circ(F) > 1$. Let $a_1, a_2, a_3, b_1, b_2, b_3 \in R$, then

$$\begin{aligned} F(a_1+a_2+a_3, b_1+b_2+b_3) &= (a_1+a_2+a_3)(b_1+b_2+b_3) = \sum_{i,j\in[3]} a_i b_j \\ &= (a_1+a_2)(b_1+b_2) + (a_1+a_3)(b_1+b_3) + (a_2+a_3)(b_2+b_3) - a_1b_1 - a_2b_2 - a_3b_3 \\ &= \sum_{j=0}^{2} \sum_{I\in\mathcal{P}_{3,j}} (-1)^{2-j} F\left(\sum_{i\in I} a_i, \sum_{i\in I} b_i\right). \end{aligned}$$

So we have that $\mathrm{d}^\circ(F) = 2$. Let $L\colon R^2 \to R$ defined by $L(a,b) = a+b$. Let $\underline{x} = (x_1, x_2, x_3, x_4) \in (R^2)^4$ where $x_i = (a_i, b_i) \in R^2$ for $i \in [4]$. Let $\mathcal{F}\colon (R^2)^4 \to R^4$ defined by in Theorem 2 with $s = d+2$, $\underline{b}$ equal to zero, and $P_j = L$ for $j \in [4]$. So $\mathcal{F}(\underline{x})$ is equal to

$$\begin{pmatrix} L(a_1,b_1) \\ L(a_2,b_2) + F\left(\sum_{i\in[2,4]} a_i, \sum_{i\in[2,4]} b_i\right) \\ L(a_3,b_3) + F\left(a_1 + \sum_{i\in[3,4]} a_i, b_1 + \sum_{i\in[3,4]} b_i\right) - F\left(\sum_{i\in[3,4]} a_i, \sum_{i\in[3,4]} b_i\right) \\ \sum_{I\in\mathcal{P}_2} (-1)^{2-|I|} F\left(\sum_{i\in I} a_i, \sum_{i\in I} b_i\right) - L(a_1,b_1) - L(a_2,b_2) - L(a_3,b_3) \end{pmatrix}$$

and to

$$\begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 + \sum_{i,j\in[2,4]} a_i b_j \\ a_3 + b_3 + a_1b_1 + a_1b_3 + a_1b_4 + a_3b_1 + a_4b_1 \\ a_1b_2 + a_2b_1 - a_1 - a_2 - a_3 - b_1 - b_2 - b_3 \end{pmatrix}.$$

6 On the Integer-Valued (IV) polynomial representation

In this section, we provide more tools to compute the functional degree of a given function between finite Abelian groups. Then we introduce the IV polynomial representation for such functions. At the end, we compute the functional degree and the IV polynomial representation of conversion maps between $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$.

6.1 The partial degree

A useful notion is the one of *partial degree* introduced in section 5 of [AM21].

Definition 8. Let $F\colon \prod_{i\in[n]} \mathbb{X}_i \to \mathbb{Y}$ where $\mathbb{X}_1, \ldots, \mathbb{X}_n, \mathbb{Y}$ are Abelian groups. Then the partial degree of F in $i \in [n]$ is defined by

$$\mathrm{d}_i^\circ(F) = \sup(\{\mathrm{d}^\circ(F \circ \iota_{i,b})\colon b \in \mathbb{X}\})$$

where $\iota_{i,b}\colon \mathbb{X}_i \to \mathbb{X}$ is defined by $a \mapsto (b_1, \ldots, b_{i-1}, a, b_{i+1}, \ldots, b_n)$.

A simple observation is the following proposition.

Proposition 7. *Let $F\colon \prod_{i\in[n]} \mathbb{X}_i \to \mathbb{Y}$ where $\mathbb{X}_1, \ldots, \mathbb{X}_n, \mathbb{Y}$ are Abelian groups. Then we have that*

$$\mathrm{d}_i^\circ(F) = \inf(\{d \in \mathbb{N} \mid \partial_a^{i,(d+1)} F = 0 \text{ for all } a \in \mathbb{X}_i\}).$$

Proof. Let $b \in \mathbb{X}$ and $\iota_{i,b}$ as in Definition 8. For any $a, x_i \in \mathbb{X}_i$ we have that $\Delta_a(F \circ \iota_{i,b})(x_i) = \partial^i_a F(x)$ where $x = \iota_{i,b}(x_i)$. This concludes the proof since for any $x \in \prod_{i\in[n]} \mathbb{X}_i$ we have that $x = \iota_{i,x}(x_i)$ where $x = (x_1, \dots, x_n) \in \prod_{i\in[n]} \mathbb{X}_i$. □

The notion of partial degree can be used to estimate the functional degree of F.

Proposition 8 ([AM21, Theorem 5.2])**.** *Let $F\colon \prod_{i\in[n]} \mathbb{X}_i \to \mathbb{Y}$ where $\mathbb{X}_1, \dots, \mathbb{X}_n, \mathbb{Y}$ are Abelian groups. Then we have that*

$$\mathrm{d}^\circ_{i'}(F) \le \mathrm{d}^\circ(F) \le \sum_{i\in[n]} \mathrm{d}^\circ_i(F)$$

for any $i' \in [n]$.

Computing the functional degree by applying directly Definition 6 could be computationally challenging. Fortunately, [AM21, Lemma 2.2] provides a way to simplify such problem. Let $A \subseteq \mathbb{X}$ be a generator set of $\mathbb{X}$, then it is enough to verify Fréchet's equation (5) for all $\underline{a} \in A^{d+1}$. We are interested in the case where $\mathbb{X} = \mathbb{Z}^n$.

Lemma 6. *Let $\mathbb{Y}$ be an Abelian group and $P\colon \mathbb{Z}^n \to \mathbb{Y}$. Then we have the following.*

1. *For any $d \in \mathbb{N}$, we have that $\mathrm{d}^\circ(P) \le d$ if and only if $\partial^{(\underline{d})} P = 0$ for all $\underline{d} \in \mathbb{N}^n$ such that $\sum_{i\in[n]} d_i = d + 1$.*
2. *For any $i \in [n]$ and any $d \in \mathbb{N}$, we have that $\mathrm{d}^\circ_i(P) \le d$ if and only if $\partial^{i,(d+1)} P = 0$.*
3. *If for all $i \in [n]$ we have $\partial^i P = 0$, then P is constant.*

Proof. Let us prove 1. By using [AM21, Lemma 2.2], we can take $A = \{e_1, \dots, e_n\}$ where $e_i = (e_{i,1}, \dots, e_{i,n}) \in \mathbb{Z}^n$ and $e_{i,j} = 0$ if $i \neq j$ and $e_{i,i} = 1$. Then we have that $\Delta_{e_i} F = \partial^i F$.

To prove 2, it is enough to use item 1 and the characterization of the partial degree given in Proposition 7.

Let us prove 3. Consider the case $n = 1$. If $\partial^1 P = \Delta P = 0$, then $P(x + 1) = P(x)$ for all $x \in \mathbb{Z}$. Since $\mathbb{Z}$ is generated by 1, this implies that $P(x) = P(0)$ for all $x \in \mathbb{Z}$. Therefore, we have that P is constant. If $n > 1$, then each of the condition $\partial^i P = 0$ for some $i \in [n]$ implies that P does not depend on its i-th coordinate. Therefore, we have that P is constant. □

6.2 The IV polynomial representation

We present the connection between IV polynomials and the functional degree. This has been presented in [CS23], but we give an original self-contained presentation to guide the reader. We will often consider IV polynomials as functions without specifying it.

Lemma 7. *Let $\underline{d} \in \mathbb{N}^n$, then we have that $\mathrm{d}^\circ \binom{x_1,\dots,x_n}{d_1,\dots,d_n} = \sum_{i\in[n]} d_i$ and $\mathrm{d}^\circ_i \binom{x_1,\dots,x_n}{d_1,\dots,d_n} = d_i$ for all $i \in [n]$.*

Proof. Let $d \in \mathbb{N}$, observe that $\Delta\binom{x}{d} = \binom{x+1}{d} - \binom{x}{d} = \binom{x}{d-1}$ by Pascal's rule. Then $\Delta^{(k)}\binom{x}{d} = \binom{x}{d-k}$ for any $k \in \mathbb{N}$. Similarly for any $\underline{d}, \underline{k} \in \mathbb{N}^n$, we have that

$$\partial^{(\underline{k})} \binom{x_1, \dots, x_n}{d_1, \dots, d_n} = \prod_{i\in[n]} \binom{x}{d_i - k_i}.$$

If $\sum_{i\in[n]} k_i \le \sum_{i\in[n]} d_i$ then there is a choice of $\underline{k} \in \mathbb{N}^n$ such that $k_i \le d_i$ for all $i \in [n]$ and therefore $\partial^{(\underline{k})} \binom{x_1,\dots,x_n}{d_1,\dots,d_n} \neq 0$. If $\sum_{i\in[n]} k_i = \sum_{i\in[n]} d_i + 1$, then there exists $i \in [n]$ such that $k_i > d_i$ and therefore $\partial^{(\underline{k})} \binom{x_1,\dots,x_n}{d_1,\dots,d_n} = 0$. So we have that $\mathrm{d}^\circ \binom{x_1,\dots,x_n}{d_1,\dots,d_n} = \sum_{i\in[n]} d_i$. Similarly, we have that $\mathrm{d}^\circ_i \binom{x_1,\dots,x_n}{d_1,\dots,d_n} = d_i$ for all $i \in [n]$. □

Definition 9 (IV polynomial representation)**.** Let $\mathbb{Y}$ be an Abelian group and let $P\colon \mathbb{Z}^n \to \mathbb{Y}$. We say that P admits an IV polynomial representation if we can write P as

$$P(x_1,\dots,x_n) = \sum_{\underline{d}\in\mathbb{N}^n} \partial^{(\underline{d})}P(0)\binom{x_1,\dots,x_n}{d_1,\dots,d_n}$$

and $\partial^{(\underline{d})}P(0) \neq 0$ only for finitely many $\underline{d} \in \mathbb{N}^n$.

Lemma 8. *Let $\mathbb{Y}$ be an Abelian group and $P\colon \mathbb{Z}^n \to \mathbb{Y}$ with $\mathrm{d}^\circ(P) < \infty$. Then we have that*

$$\mathrm{d}^\circ(P) = \sup\left\{\sum_{i\in[n]} d_i \colon \partial^{(\underline{d})}P(0) \neq 0\right\}$$

and that

$$\mathrm{d}_i^\circ(P) = \sup\{d \in \mathbb{N} \mid \partial^{i,(d)}P(0) \neq 0\}.$$

Proof. Let $d = \mathrm{d}^\circ(P)$ and let $d' = \sup\{\sum_{i\in[n]} d_i \colon \partial^{(\underline{d})}P(0) \neq 0\}$. Then we have that $d' \leq d$. Suppose that $d' < d$ and let $\underline{d} \in \mathbb{N}^n$ be such that $\sum_{i\in[n]} d_i = d$. We have that $Q = \partial^{(\underline{d})}P$ is constant by item 3 of Lemma 6 and $Q(0) = 0$ by hypothesis. Therefore, we have $Q = 0$. So we have that $\mathrm{d}^\circ(P) < d$ by item 1 of Lemma 6 and this is a contradiction.

Let $i \in [n]$. Since $\mathrm{d}^\circ(P) < \infty$, then $\mathrm{d}_i^\circ(P) < \infty$. Similarly as before, we have that $\mathrm{d}_i^\circ(P) = \sup\{d \colon \partial^{i,(d)}P(0) \neq 0\}$. □

Proposition 9. *Let $\mathbb{Y}$ be an Abelian group and let $P\colon \mathbb{Z}^n \to \mathbb{Y}$. Then $\mathrm{d}^\circ(P) < \infty$ if and only if P admits an IV polynomial representation. Moreover, $\mathrm{d}^\circ(P)$ is equal to the degree of the IV polynomial.*

Proof. By construction, we already know that if P admits an IV polynomial representation, then $\mathrm{d}^\circ(P) < \infty$.

Suppose that $\mathrm{d}^\circ(P) < \infty$, then $\partial^{(\underline{d})}P(0) \neq 0$ only for finitely many $\underline{d} \in \mathbb{N}^n$. Let

$$\bar{P}(x_1,\dots,x_n) = \sum_{\underline{d}\in\mathbb{N}^n} \partial^{(\underline{d})}P(0)\binom{x_1,\dots,x_n}{d_1,\dots,d_n},$$

then for any $\underline{k} \in \mathbb{N}^n$ we have that

$$\begin{aligned}\partial^{(\underline{k})}(P-\bar{P})(0) &= \partial^{(\underline{k})}P(0) - \sum_{\underline{d}\in\mathbb{N}^n} \partial^{(\underline{d})}P(0)\prod_{i\in[n]}\binom{0}{d_i-k_i}\\ &= \partial^{(\underline{k})}P(0) - \partial^{(\underline{k})}P(0) = 0.\end{aligned}$$

By Lemma 8, we can conclude that $\mathrm{d}^\circ(P-\bar{P}) = 0$ and that $P - \bar{P}$ is constant. Since $\bar{P}(0) = \partial^{(\underline{0})}P(0) = P(0)$, we have that $P = \bar{P}$. □

Let $\mathbb{Y}$ be an Abelian group and $\mathbb{X} = \prod_{i\in[n]} \mathbb{Z}_{q_i}$ for some $q_i \in \mathbb{N}$ where we recall that $\mathbb{Z}_0 = \mathbb{Z}$ and $\mathbb{Z}_1 = \{0\}$. We say that $P\colon \mathbb{Z}^n \to \mathbb{Y}$ is the pullback of a function $F\colon \mathbb{X} \to \mathbb{Y}$ if $P = F \circ \varepsilon$ where $\varepsilon\colon \mathbb{Z}^n \to \mathbb{X}$ defined by

$$\varepsilon(x_1,\dots,x_n) = (x_1 + q_1\mathbb{Z},\dots,x_n + q_n\mathbb{Z}). \tag{9}$$

Proposition 10. *Let $\mathbb{Y}$ be an Abelian group and $\mathbb{X} = \prod_{i\in[n]} \mathbb{Z}_{q_i}$ for some $q_i \in \mathbb{N}$. Let $F\colon \mathbb{X} \to \mathbb{Y}$ and $P\colon \mathbb{Z}^n \to \mathbb{Y}$ be the pullback of F. Then $\mathrm{d}^\circ(F) = \mathrm{d}^\circ(P)$.*

Proof. Let $\varepsilon\colon \mathbb{Z}^n \to \mathbb{X}$ be as in (9). It is clear that if F is constant, then P is also constant and so they have the same functional degree 0. Suppose that F is not constant. Let $d \in \mathbb{N}$, $\underline{a} = (a_1, \dots, a_{d+1}) \in \mathbb{X}^{d+1}$, and $x \in \mathbb{X}$ such that $\Delta^{(d+1)}_{\underline{a}} F(x) \neq 0$. Let $x' \in \mathbb{Z}^n$ and $\underline{a}' = (a'_1, \dots, a'_{d+1}) \in (\mathbb{Z}^n)^{d+1}$ be such that $\varepsilon(x') = x$ and $\varepsilon(a'_i) = a_i$ for $i \in [n]$. Then we have that $\Delta^{(d+1)}_{\underline{a}'} P(x') \neq 0$. So we have that $\mathrm{d}^\circ(F) \leq \mathrm{d}^\circ(P)$. So if $\mathrm{d}^\circ(F) = \infty$, then $\mathrm{d}^\circ(P) = \infty$. If $\mathrm{d}^\circ(F) < \infty$, then by [AM21, Theorem 4.3], we have that $\mathrm{d}^\circ(P) = \mathrm{d}^\circ(F \circ \varepsilon) \leq \mathrm{d}^\circ(F) \cdot \mathrm{d}^\circ(\varepsilon) = \mathrm{d}^\circ(F)$ because $\mathrm{d}^\circ(\varepsilon) = 1$. □

6.3 On the functions of the form $f\colon \prod_{i\in[n]} \mathbb{Z}_{p^{\alpha_i}} \to \mathbb{Z}_{p^\beta}$

By Proposition 6, we have that to study all the functions with finite functional degree and between finitely generated Abelian groups, it is enough to consider functions of the form $f\colon \prod_{i\in[n]} \mathbb{Z}_{p^{\alpha_i}} \to \mathbb{Z}_{p^\beta}$. In [CS22], the author proves the best possible upper bound for such functions.

Proposition 11 ([CS22, Theorem 4.9])**.** *Let p be prime and $\alpha_1, \dots, \alpha_n, \beta$ be positive integers. Let $\delta_p(\underline{\alpha}, \beta) = \sum_{i\in[n]} p^{\alpha_i} - n + (\beta - 1)(p-1)p^{\alpha_{\max}-1}$ where $\alpha_{\max} = \max_{i\in[n]} \alpha_i$. Then the best upper bound of the functional degree of any $f\colon \prod_{i\in[n]} \mathbb{Z}_{p^{\alpha_i}} \to \mathbb{Z}_{p^\beta}$ is given by*

$$\mathrm{d}^\circ(f) \leq \delta_p(\underline{\alpha}, \beta)$$

and it is reached if f is the function defined by $f(x) = 1$ if $x = 0$ and $f(x) = 0$ otherwise.

Observe that the bound in Proposition 11 also holds for functions $f\colon \mathbb{F}_p^n \to \mathbb{F}_p$ since $\delta_p(\underline{1}, 1) = n(p-1)$.

To conclude, we show that for any function $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ there is an IV polynomial representation that coincides with its algebraic normal form (1).

Proposition 12. *Let p be a prime and $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$. Then the IV polynomial representation of F coincides with its algebraic normal form (1).*

Proof. Let $P = F \circ \varepsilon$ be the pullback of F where ε is defined by in (9). For $i \in [n]$, we have that $\mathrm{d}^\circ_i(P) = \mathrm{d}^\circ_i(F) \leq \delta_p(1, 1) = p - 1$ by the bound in Proposition 11. So we have that

$$P(x_1, \dots, x_n) = \sum_{\underline{d}\in\{0,\dots,p-1\}^n} P_{\underline{d}} \binom{x_1, \dots, x_n}{d_1, \dots, d_n},$$

where $P_{\underline{d}} \in \mathbb{F}_p^m$. Let $d \in \{1, \dots, p-1\}$, then

$$\binom{x}{d} = \frac{x(x-1)\cdots(x-d+1)}{d!} = (d!)^{-1} x(x-1)\cdots(x-d+1) \in \mathbb{F}_p[x]$$

because $d! \in \mathbb{F}_p \setminus \{0\}$. So, for any $\underline{d} \in \{0, \dots, p-1\}^n$ we have that

$$\binom{x_1, \dots, x_n}{d_1, \dots, d_n} = \prod_{i\in[n]\colon d_i\neq 0} (d_i!)^{-1} x_i(x_i - 1)\cdots(x_i - d_i + 1).$$

Let $\lambda\colon \mathbb{F}_p^n \to \mathbb{Z}^n$ be an injective homomorphism such that $\varepsilon \circ \lambda$ is the identity over $\mathbb{F}_p^n$. Since $P \circ \lambda = F \circ \varepsilon \circ \lambda = F$, then we can conclude the proof by the uniqueness of the ANF. □

6.4 The Integer-Valued (IV) polynomial representations of conversion maps between $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$

Let p be a prime and n be a positive integer. We consider the conversion map $\mathbb{Z}_{p^n} \to \mathbb{F}_p^n$ and its inverse with particular interest for the case $p = 2$. By computing the functional degree, we quantify the amount of shares that are necessary to convert from a Boolean sharing to an arithmetic sharing and viceversa.

We recall that since $\mathbb{Z}_p = \mathbb{F}_p$, then $\mathbb{F}_p^n = \mathbb{Z}_p^n$, but $\mathbb{Z}_p^n \neq \mathbb{Z}_{p^n}$ for $n \geq 2$. For clarity, we will write any element of $\mathbb{Z}_{p^n}$ in the form $x + p^n\mathbb{Z}$ where $x \in \{0, \dots, p^n - 1\} \subseteq \mathbb{Z}$ and any element of $\mathbb{F}_p^n$ in the form $(x_1 + p\mathbb{Z}, \dots, x_n + p\mathbb{Z})$ where $(x_1, \dots, x_n) \in \{0, \dots, p-1\}^n \subseteq \mathbb{Z}^n$.

We consider the natural conversion map from $\tau^{(n)} \colon \mathbb{Z}_{p^n} \to \mathbb{F}_p^n$ that takes $x + p^n\mathbb{Z}$ with $x \in \{0, \dots, p^n - 1\}$, its p-adic expansion $x = \sum_{i\in[n]} x_i p^{i-1}$ with $x_i \in \{0, \dots, p-1\}$ and maps it to $(x_1 + p\mathbb{Z}, \dots, x_n + p\mathbb{Z}) \in \mathbb{F}_p^n$. In order to show the IV polynomial representation of $\tau^{(n)}$ we need to prove the following lemma which is a consequence of the Lucas Theorem (see Subsection 2.3).

Lemma 9. *Let $x \in \mathbb{Z}$ and let $(x_1, \dots, x_n) \in \{0, \dots, p-1\}^n \subseteq \mathbb{Z}^n$ be such that $x = \sum_{i\in[n]} x_i p^{i-1} \pmod{p^n}$. Then we have that*

$$\binom{x}{p^{j-1}} = x_j \pmod{p}$$

for any $j \in [n]$.

Proof. The proof is in Appendix A.2 □

Remark 8. Digit extraction is an important step in the bootstrapping for the Homomorphic Encryption scheme BGV and BFV [GV23]. It consists in taking a positive integer x, its p-adic expansion $\sum_{i\in[n]} x_i p^{i-1}$ and compute directly some x_j by using only addition, multiplications and modulo reductions on x. In [GIKV23], they approach this problem by using "polyfunctions" which are polynomials in $\mathbb{Z}_{p^n}[x]$ represented using the factorial basis $\{x(x-1)\cdots(x-d+1)\}_{d\in\mathbb{N}}$. These representation is closely releted to the IV polynomial representation since $\binom{x}{d} = \frac{x(x-1)\cdots(x-d+1)}{d!}$.

Let $\tau^{(n)} \colon \mathbb{Z}_{p^n} \to \mathbb{F}_p^n$ be defined by

$$x = \sum_{i\in[n]} x_i p^{i-1} + p^n\mathbb{Z} \mapsto \tau^{(n)}(x) = (x_1 + p\mathbb{Z}, \dots, x_n + p\mathbb{Z})$$

where $(x_1, \dots, x_n) \in \{0, \dots, p-1\}^n \subseteq \mathbb{Z}^n$.

Proposition 13. *Let p be a prime number and n a positive integer. Let $e_i \in \mathbb{F}_p^n$ be the vector of all zeroes except for the i-th coordinate which is equal to $1 + p\mathbb{Z}$. Then the IV polynomial representation of $\tau^{(n)}$ is given by*

$$\tau^{(n)}(x) = \sum_{i\in[n]} e_i \binom{x}{p^{i-1}}$$

and we have that $\mathrm{d}^\circ(\tau^{(n)}) = p^{n-1}$.

Proof. It follows from Lemma 9. □

It is clear that the functional degree of $\tau^{(n)}$ is absurdly high for any practical application since it grows exponentially with n. We will decompose $\tau^{(n)}$ into functions of functional degree at most $(n-1)(p-1)+1$ which is clearly an improvement since it grows linearly with n. Before doing that we need to investigate the IV polynomial representation $\sigma^{(n)} = (\tau^{(n)})^{-1}$.

We need to define the following functions. Let $\chi\colon \mathbb{Z} \to \mathbb{Z}$ be the function defined by $\chi(x) = 1$ if $x = 0 \pmod p$ and $\chi(x) = 0$ otherwise. Let $\chi^{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_{p^n}$ be defined by $\chi^{(n)}(x + p\mathbb{Z}) = \chi(x) + p^n\mathbb{Z}$. Let $\omega\colon \mathbb{Z} \to \mathbb{Z}$ be such that $\omega(x) = x \mod p$ and $\omega(x) \in \{0, \dots, p-1\}$. Let $\omega^{(n)}\colon \mathbb{Z}_p \to \mathbb{Z}_{p^n}$ be defined by $\omega^{(n)}(x + p\mathbb{Z}) = \omega(x) + p^n\mathbb{Z}$.

Lemma 10. *Let p be a prime number and n a positive integer. Let k be a positive integer such that $k \le n$. Then $\mathrm{d}^\circ(p^k\chi^{(n)}) = \mathrm{d}^\circ(\chi^{(n-k)})$ and $\mathrm{d}^\circ(p^k\omega^{(n)}) = \mathrm{d}^\circ(\omega^{(n-k)})$.*

Proof. We show it for χ since the proof for ω is almost identical. Let $d \in \mathbb{N}$ then we have that that $p^k\Delta^{(d+1)}\chi^{(n)} = 0$ if and only if $p^k\Delta^{(d+1)}\chi = 0 \pmod{p^n}$ if and only if $\Delta^{(d+1)}\chi = 0 \pmod{p^{n-k}}$ if and only if $\Delta^{(d+1)}\chi^{(n-k)} = 0$. This is enough to conclude the proof. □

Lemma 11. *Let p be a prime number and n a positive integer. Then we have that $\mathrm{d}^\circ(\chi^{(n)}) = n(p-1)$ and the IV polynomial representation of $\chi^{(n)}$ is given by $\chi^{(n)}(x) = \sum_{d=0}^{n(p-1)} \chi_d\binom{x}{d}$ where*

$$\chi_d = \sum_{b=0}^{\frac{d-\omega(d)}{p}} (-1)^{d-bp}\binom{d}{bp}. \tag{10}$$

Proof. The first part is given by Proposition 11. By Equation (4), we have that

$$\chi_d = \sum_{a=0}^{d}(-1)^{d-a}\binom{d}{a}\chi(a) = \sum_{b=0}^{k}(-1)^{d-bp}\binom{d}{bp}$$

where $k \in \mathbb{N}$ is the biggest such that $kp \le d$. We conclude by observing that $d - \omega(d) = kp$. □

Lemma 12. *Let p be a prime number and n a positive integer. Then we have that $\mathrm{d}^\circ(\omega^{(n)}) = (n-1)(p-1)+1$ and the IV polynomial representation of $\omega^{(n)}$ is given by*

$$\omega^{(n)}(x) = \binom{x}{1} + \sum_{d\in[2,(n-1)(p-1)+1]} \omega_d p\binom{x}{d}$$

where $\omega_d = -\chi_d - \chi_{d-1}$ and χ_d is as in (10). In particular, if $p = 2$ we have that $\omega_d = (-1)^{d-1}2^{d-2}$.

Proof. Observe that $\mathrm{d}^\circ(\omega^{(1)}) = 1$. Suppose that $n > 1$. Observe that $\Delta\omega(x) = 1 - p$ if $x = p-1 \pmod p$ and $\Delta\omega(x) = 1$ otherwise. So we have that $\Delta\omega(x) = 1 - p\chi(x+1)$. So for any $d \in \mathbb{N}$ with $d \ge 2$ we have that $\Delta^{(d)}\omega(x) = -p\Delta^{(d-1)}\chi(x+1) = -p\Delta^{(d)}\chi(x) - p\Delta^{(d-1)}\chi(x)$. By Lemma 10, we have $\mathrm{d}^\circ(p\chi^{(n)}) = \mathrm{d}^\circ(\chi^{(n-1)})$. So we have that $\mathrm{d}^\circ(\omega^{(n)}) = \mathrm{d}^\circ(\chi^{(n-1)}) + 1$ and $\mathrm{d}^\circ(\omega^{(n)}) = (n-1)(p-1)+1$ by Proposition 11.

Suppose that $p = 2$, then $\omega(x) = \frac{1-(-1)^x}{2}$ for any $x \in \mathbb{Z}$. We claim that $\Delta^{(d)}\omega(x) = 2^{d-1}(-1)^{x+d-1}$. For $k = 1$, we have that $\Delta\omega(x) = \frac{1-(-1)^{x+1}}{2} - \frac{1-(-1)^x}{2} = (-1)^x$. Suppose the claim is true for $d \ge 1$ and let us prove it for $d+1$. We have that

$$\Delta^{(d+1)}\omega(x) = \Delta\Delta^{(d)}\omega(x) = 2^{d-1}\left((-1)^{x+d} - (-1)^{x+d-1}\right) = 2^d(-1)^{x+d}.$$

This concludes the proof because $\omega_d = \Delta^{(d)}\omega(0)/2 = 2^{d-2}(-1)^{d-1}$. □

Proposition 14. *Let p be a prime number and n a positive integer. We have that $\mathrm{d}^\circ(\sigma^{(n)}) = (n-1)(p-1)+1$ and that the IV polynomial representation of $\sigma^{(n)}$ is given by*

$$\sigma^{(n)}(x_1,\dots,x_n) = \sum_{i\in[n]} p^{i-1}\binom{x_i}{1} + \sum_{i\in[n-1]}\ \sum_{d_i\in[2,(n-i)(p-1)+1]} \omega_{d_i} p^i \binom{x_i}{d_i}.$$

where ω_d is as in Lemma 12.

Proof. Observe that $\sigma^{(n)}\colon \mathbb{F}_p^n \to \mathbb{Z}_{p^n}$ can be defined by $\sigma^{(n)}(x_1,\dots,x_n) = \sum_{i\in[n]} \omega^{(n)}(x_i)p^{i-1}$. Let $P\colon \mathbb{Z}^n \to \mathbb{Z}_{p^n}$ be the pullback of $\sigma^{(n)}$. Then the IV polynomial representation of $\sigma^{(n)}$ is equal to the IV polynomial representation of P. We observe that if $i,j\in[n]$ are such that $i\neq j$, then we have that $\partial_1^i\partial_1^j P(x) = 0$. So we have that $P(x) = \sum_{i\in[n]}\sum_{d_i\in\mathbb{N}} \left(\partial_1^{i,(d_i)}P(0)\right)\binom{x_i}{d_i} + p^n\mathbb{Z}$. So for any $i\in[n]$, we have that $\partial^{i,(d_i)}P(0) = \Delta^{(d_i)}\omega^{(n)}(0)p^{i-1}$ and that the functional degree of the map $x\mapsto \omega^{(n)}(x)p^{i-1}$ is equal to $\mathrm{d}_i^\circ(\sigma^{(n)})$. By Lemma 10, we have $\mathrm{d}^\circ(p^{i-1}\omega^{(n)}) = \mathrm{d}^\circ(\omega^{(n-i+1)})$. So we have that $\mathrm{d}_i^\circ(\sigma^{(n)}) = \mathrm{d}^\circ(\omega^{(n-i+1)})$. By Lemma 12, we have that $\mathrm{d}_i^\circ(\sigma^{(n)}) = (n-i+1)(p-1)+1$ and therefore $\mathrm{d}^\circ(\sigma^{(n)}) = (n-1)(p-1)+1$. By Lemma 12 again, we have $\Delta^{(0)}\omega^{(n)}(0)p^{i-1} = 0$, $\Delta^{(1)}\omega^{(n)}(0)p^{i-1} = p^{i-1}$, and $\Delta^{(d_i)}\omega^{(n)}(0)p^{i-1} = \omega_{d_i}p^i$. □

Instead of using the function $\tau^{(n)}$ which have high functional degree, it is possible to write it as compositions of functions with small functional degree. Let us consider $\zeta^{(n)}\colon \mathbb{Z}_{p^n}\to\mathbb{Z}_{p^{n-1}}\times\mathbb{Z}_p$ with $n\geq 2$ defined by

$$x = \sum_{i\in[n]} x_i p^{i-1} + p^n\mathbb{Z} \mapsto \zeta^{(n)}(x) = (x_1 + p\mathbb{Z}, \sum_{i\in[2,n]} x_i p^{i-2} + p^{n-1}\mathbb{Z})$$

where $(x_1,\dots,x_n)\in\{0,\dots,p-1\}^n\subseteq\mathbb{Z}^n$. By Lemma 9, we have that the IV polynomial representation of $\zeta^{(n)}$ is

$$\zeta^{(n)}(x) = \binom{x}{1}e_1 + \eta^{(n)}(x)e_2$$

where $e_1 = (1+p\mathbb{Z}, 0+p^{n-1}\mathbb{Z})$, $e_2 = (0+p\mathbb{Z}, 1+p^{n-1}\mathbb{Z})$, and $\eta^{(n)}\colon\mathbb{Z}_{p^n}\to\mathbb{Z}_{p^{n-1}}$ defined by

$$x = \sum_{i\in[n]} x_i p^{i-1} + p^n\mathbb{Z} \mapsto \eta^{(n)}(x) = \sum_{i\in[2,n]} x_i p^{i-2} + p^{n-1}\mathbb{Z}$$

where $(x_1,\dots,x_n)\in\{0,\dots,p-1\}^n\subseteq\mathbb{Z}^n$. So we can write

$$\begin{aligned} x &\xmapsto{\zeta^{(n)}} \left(\binom{x}{1}, \eta^{(n)}(x)\right) \xmapsto{(\mathrm{id}_{\mathbb{Z}_p},\zeta^{(n-1)})} \left(\binom{x}{1}, \binom{\eta^{(n)}(x)}{1}, \eta^{(n-1)}(\eta^{(n)}(x))\right) \\ &= \left(\binom{x}{1}, \binom{x}{2}, \eta^{(n-1)}(\eta^{(n)}(x))\right) \xmapsto{(\mathrm{id}_{\mathbb{Z}_p},\mathrm{id}_{\mathbb{Z}_p},\zeta^{(n-2)})} \cdots \xmapsto{(\mathrm{id}_{\mathbb{Z}_p},\dots,\mathrm{id}_{\mathbb{Z}_p},\zeta^{(2)})} \tau^{(n)}(x). \end{aligned}$$

By using the IV polynomial representation of $\zeta^{(n)}$, we have that $\mathrm{d}^\circ(\zeta^{(n)}) = \mathrm{d}^\circ(\eta^{(n)})$ because $\eta^{(n)}$ is not a constant function.

Proposition 15. *Let p be a prime number and n a positive integer. We have that $\mathrm{d}^\circ(\eta^{(n)}) = (n-1)(p-1)+1$ and that the IV polynomial representation of $\eta^{(n)}$ is given by*

$$\eta^{(n)}(x) = \sum_{d\in[2,(n-1)(p-1)+1]} (-\omega_d)\binom{x}{d}$$

where ω_d is as in Lemma 12.

Proof. We observe that $\eta^{(n)}(x) = \sigma^{(n-1)}\left(\binom{x}{p}, \binom{x}{p^2}, \ldots, \binom{x}{p^{n-1}}\right)$ and therefore

$$\eta^{(n)}(x) = \sum_{i\in[n-1]} p^{i-1}\begin{pmatrix}\binom{x}{p^i}\\ 1\end{pmatrix} + \sum_{i\in[n-2]}\sum_{d_i\in[2,(n-i-1)(p-1)+1]} \omega_d p^i \begin{pmatrix}\binom{x}{p^i}\\ d_i\end{pmatrix}$$

by Proposition 14. Observe that the following holds:

$$\begin{aligned}\eta^{(n)}(x) - \sum_{d\in[2,(n-1)(p-1)+1]} (-\omega_d)\binom{x}{d} &= \eta^{(n)}(x) + \sum_{d_0\in[2,n]} \omega_{d_0}\begin{pmatrix}\binom{x}{1}\\ d_0\end{pmatrix}\\ = \sum_{i\in[n-1]} p^{i-1}\binom{x}{p^i} + \sum_{i=0}^{n-2}\sum_{d_i\in[2,(n-i-1)(p-1)+1]} \omega_{d_i} p^i \begin{pmatrix}\binom{x}{p^i}\\ d_i\end{pmatrix} &\pmod{p^{n-1}}.\end{aligned}$$

Since $\sigma^{(n)}\circ\tau^{(n)}$ is the identity function, we have that the following holds:

$$\begin{aligned}\binom{x}{1} &= \sum_{i\in[n]} p^{i-1}\begin{pmatrix}\binom{x}{p^{i-1}}\\ 1\end{pmatrix} + \sum_{i\in[n-1]}\sum_{d_i'\in[2,(n-i)(p-1)+1]} \omega_{d_i'} p^i \begin{pmatrix}\binom{x}{p^{i-1}}\\ d_i'\end{pmatrix} &\pmod{p^n}\\
\binom{x}{1} &= \sum_{i\in[n]} p^{i-1}\binom{x}{p^{i-1}} + \sum_{i\in[n-1]}\sum_{d_i'\in[2,(n-i)(p-1)+1]} \omega_{d_i'} p^i \begin{pmatrix}\binom{x}{p^{i-1}}\\ d_i'\end{pmatrix} &\pmod{p^n}\\
0 &= \sum_{i\in[n-1]} p^i\binom{x}{p^i} + \sum_{i=0}^{n-2}\sum_{d_i\in[2,(n-i-1)(p-1)+1]} \omega_{d_i} p^{i+1}\begin{pmatrix}\binom{x}{p^i}\\ d_i\end{pmatrix} &\pmod{p^n}\\
0 &= p\left(\sum_{i\in[n-1]} p^{i-1}\binom{x}{p^i} + \sum_{i=0}^{n-2}\sum_{d_i\in[2,(n-i-1)(p-1)+1]} \omega_{d_i} p^i \begin{pmatrix}\binom{x}{p^i}\\ d_i\end{pmatrix}\right) &\pmod{p^n}\\
0 &= \sum_{i\in[n-1]} p^{i-1}\binom{x}{p^i} + \sum_{i=0}^{n-2}\sum_{d_i\in[2,(n-i-1)(p-1)+1]} \omega_{d_i} p^i \begin{pmatrix}\binom{x}{p^i}\\ d_i\end{pmatrix} &\pmod{p^{n-1}}.\end{aligned}$$

This concludes the proof. □

Acknowledgements We thank Siemen Dhooghe and Svetla Nikova for useful discussions.

References

[AM21] Erhard Aichinger and Jakob Moosbauer. Chevalley-warning type results on abelian groups. *Journal of Algebra*, 569:30–66, 2021.

[BBS17] Dusan Bozilov, Begül Bilgin, and Haci Ali Sahin. A note on 5-bit quadratic permutations' classification. *IACR Trans. Symmetric Cryptol.*, 2017(1):398–404, 2017.

[BFG15] Josep Balasch, Sebastian Faust, and Benedikt Gierlichs. Inner product masking revisited. In *Advances in Cryptology–EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I 34*, pages 486–510. Springer, 2015.

[BGN+15] Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Trade-offs for threshold implementations illustrated on AES. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 34(7):1188–1200, 2015.

[BNN+12] Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, and Georg Stütz. Threshold implementations of all 3 ×3 and 4 ×4 s-boxes. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 76–91. Springer, 2012.

[Bou22] Chad Boutin. Nist announces first four quantum-resistant cryptographic algorithms. *National Institute of Standards and Technology*, 2022.

[CC97] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48. American Mathematical Soc., 1997.

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, 1999.

[CMM+23] Gaëtan Cassiers, Loïc Masure, Charles Momin, Thorben Moos, and François-Xavier Standaert. Prime-field masking in hardware and its soundness against low-noise sca attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 482–518, 2023.

[CPRR15] Claude Carlet, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Algebraic decomposition for probing security. In *CRYPTO (1)*, volume 9215 of *Lecture Notes in Computer Science*, pages 742–763. Springer, 2015.

[CS22] Pete L Clark and Uwe Schauz. Functional degrees and arithmetic applications i: The set of functional degrees. *Journal of Algebra*, 608:691–718, 2022.

[CS23] Pete L Clark and Uwe Schauz. Functional degrees and arithmetic applications ii: The group-theoretic prime ax-katz theorem. *arXiv preprint arXiv:2305.01304*, 2023.

[DNR19] Siemen Dhooghe, Svetla Nikova, and Vincent Rijmen. Threshold implementations in the robust probing model. In Begül Bilgin, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Proceedings of ACM Workshop on Theory of Implementation Security, TIS@CCS 2019, London, UK, November 11, 2019*, pages 30–37. ACM, 2019.

[GIKV23] Robin Geelen, Ilia Iliashenko, Jiayi Kang, and Frederik Vercauteren. On polynomial functions modulo pe and faster bootstrapping for homomorphic encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 257–286. Springer, 2023.

[Gou01] Louis Goubin. A sound method for switching between boolean and arithmetic masking. In *Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3*, pages 3–15. Springer, 2001.

[GP99] Louis Goubin and Jacques Patarin. DES and differential power analysis (the "duplication" method). In Çetin Kaya Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, volume 1717 of *Lecture Notes in Computer Science*, pages 158–172. Springer, 1999.

[GV23] Robin Geelen and Frederik Vercauteren. Bootstrapping for bgv and bfv revisited. *Journal of Cryptology*, 36(2):12, 2023.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology - CRYPTO '99 Proceedings*, pages 388–397, 1999.

[Lac04] Miklós Laczkovich. Polynomial mappings on abelian groups. *aequationes mathematicae*, 68:177–199, 2004.

[MPO05] Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. Successfully attacking masked AES hardware implementations. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 157–171. Springer, 2005.

[NRR06] Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold implementations against side-channel attacks and glitches. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *Information and Communications Security, 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006, Proceedings*, volume 4307 of *Lecture Notes in Computer Science*, pages 529–545. Springer, 2006.

[PAB+23] Enrico Piccione, Samuele Andreoli, Lilya Budaghyan, Claude Carlet, Siemen Dhooghe, Svetla Nikova, George Petrides, and Vincent Rijmen. An optimal universal construction for the threshold implementation of bijective s-boxes. *IEEE Transactions on Information Theory*, 2023.

[Sch14] Uwe Schauz. Classification of polynomial mappings between commutative groups. *Journal of Number Theory*, 139:1–28, 2014.

A Appendix

A.1 Proof of Proposition 5

Proof. Let $s \geq d+1$ and $x_1, \ldots, x_s \in \mathbb{X}$. By using Lemma 2, we know that if the functional expansion (6) holds then F has functional degree at most d. We claim that if F has functional degree at most d, then the functional expansion (6) holds. The case $s = d+1$ is exactly the expression given by 2 in Lemma 2 because $\mu_{d+1,d}(j) = (-1)^{d-j}\binom{d-j}{d-j} = (-1)^{d-j}$. We continue the proof by induction on s. Let $x_1, \ldots, x_{s+1} \in \mathbb{X}$. We defin

Set $z_i = x_i$ for $i \in [s-1]$ and $z_s = x_s + x_{s+1}$. By using the induction hypothesis, we have that

$$
\begin{aligned}
&F\left(\sum_{i\in[s+1]} x_i\right) = F\left(\sum_{i\in[s]} z_i\right) = \sum_{j=0}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s,j}} F\left(\sum_{i\in I} z_i\right) \\
&= \sum_{j=0}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s-1,j}} F\left(\sum_{i\in I} z_i\right) + \sum_{j=1}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s-1,j-1}} F\left(\sum_{i\in I} z_i + z_s\right) \\
&= \sum_{j=0}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s-1,j}} F\left(\sum_{i\in I} x_i\right) + \sum_{j=1}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s-1,j-1}} F\left(\sum_{i\in I} x_i + x_s + x_{s+1}\right)
\end{aligned}
$$

We continue by decomposing the second term of the last expression. We have that

$$\begin{aligned}
&\sum_{j=1}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s-1,j-1}} F\left(\sum_{i\in I} x_i + x_s + x_{s+1}\right) \\
&= \sum_{j=2}^{d} \mu_{s,d}(j-1) \sum_{I\in\mathcal{P}_{s-1,j-2}} F\left(\sum_{i\in I} x_i + x_s + x_{s+1}\right) + \sum_{I\in\mathcal{P}_{s-1,d-1}} F\left(\sum_{i\in I} x_i + x_s + x_{s+1}\right)
\end{aligned}$$

because $\mu_{s,d}(d) = 1$.

We continue by considering the second term of the last expression. By Lemma 2, we have that

$$\begin{aligned}
\sum_{I\in\mathcal{P}_{s-1,d-1}} F\left(\sum_{i\in I} x_i + x_s + x_{s+1}\right) &= \sum_{I\in\mathcal{P}_{s-1,d-1}} \sum_{j=0}^{d} (-1)^{d-j} \sum_{J\subseteq I\cup\{s,s+1\}\colon |J|=j} F\left(\sum_{i\in J} x_i\right) \\
&= \sum_{j=0}^{d} (-1)^{d-j} \sum_{J\in\mathcal{P}_{s+1,j}} \sum_{\substack{I\in\mathcal{P}_{s-1,d-1} \\ J\subseteq I\cup\{s,s+1\}}} F\left(\sum_{i\in J} x_i\right) \\
&= \sum_{j=0}^{d} (-1)^{d-j} \sum_{I\in\mathcal{P}_{s+1,j}} \sum_{\substack{J\in\mathcal{P}_{s-1,d-1} \\ I\subseteq J\cup\{s,s+1\}}} F\left(\sum_{i\in I} x_i\right)
\end{aligned}$$

Let $j \in \{0,\dots,d\}$ and let $I \in \mathcal{P}_{s+1,j}$. Let us count the number of $J \in \mathcal{P}_{s-1,d-1}$ such that $I \subseteq J \cup \{s, s+1\}$. We have 4 cases:

Case $s, s+1 \notin I$: In this case, $j \leq d-1$ and we have to count the number of subsets of $[s-1] \setminus I$ with cardinality $d-j-1$. That is $\binom{s-j-1}{d-j-1}$.

Case $s \in I$ and $s+1 \notin I$: In this case, we have to count the number of subsets of $[s-1] \setminus (I \setminus \{s\})$ with cardinality $(d-1)-(j-1)$. That is $\binom{s-j}{d-j}$.

Case $s \notin I$ and $s+1 \in I$: Similarly to the previous case, it is $\binom{s-j}{d-j}$.

Case $s, s+1 \in I$: In this case, we have to count the number of subsets of $[s-1] \setminus (I \setminus \{s, s+1\})$ with cardinality $(d-1)-(j-2)$. That is $\binom{s-j+1}{d-j+1}$.

So we have that

$$\begin{aligned}
&\sum_{j=0}^{d} (-1)^{d-j} \sum_{I\in\mathcal{P}_{s+1,j}} \sum_{\substack{J\in\mathcal{P}_{s-1,d-1} \\ I\subseteq J\cup\{s,s+1\}}} F\left(\sum_{i\in I} x_i\right) = \\
&= \sum_{j=0}^{d-1} (-1)^{d-j} \binom{s-j-1}{d-j-1} \sum_{I\in\mathcal{P}_{s-1,j}} F\left(\sum_{i\in I} x_i\right) \\
&\quad + \sum_{j=1}^{d} (-1)^{d-j} \binom{s-j}{d-j} \sum_{I\in\mathcal{P}_{s-1,j-1}} \left(F\left(\sum_{i\in I} x_i + x_s\right) + F\left(\sum_{i\in I} x_i + x_{s+1}\right)\right) \\
&\quad + \sum_{j=2}^{d} (-1)^{d-j} \binom{s-j+1}{d-j+1} \sum_{I\in\mathcal{P}_{s-1,j-2}} F\left(\sum_{i\in I} x_i + x_s + x_{s+1}\right).
\end{aligned}$$

Observe that $(-1)^{d-j}\binom{s-j-1}{d-j-1} = -\mu_{s+1,d}(j+1)$, that $(-1)^{d-j}\binom{s-j}{d-j} = \mu_{s+1,d}(j)$, and that

$(-1)^{d-j}\binom{s-j+1}{d-j+1} = -\mu_{s+1,d}(j-1)$. So we have that $F\left(\sum_{i\in[s+1]} x_i\right)$ is equal to

$$\sum_{j=0}^{d-1}(\mu_{s,d}(j)-\mu_{s+1,d}(j+1))\sum_{I\in\mathcal{P}_{s-1,j}} F\left(\sum_{i\in I} x_i\right)+\mu_{s,d}(d)\sum_{I\in\mathcal{P}_{s-1,d}} F\left(\sum_{i\in I} x_i\right)$$
$$+\sum_{j=1}^{d}(-1)^{d-j}\mu_{s+1,d}(j)\sum_{I\in\mathcal{P}_{s-1,j-1}}\left(F\left(\sum_{i\in I} x_i+x_s\right)+F\left(\sum_{i\in I} x_i+x_{s+1}\right)\right)$$
$$+\sum_{j=2}^{d}(\mu_{s,d}(j-1)-\mu_{s+1,d}(j-1))\sum_{I\in\mathcal{P}_{s-1,j-2}} F\left(\sum_{i\in I} x_i+x_s+x_{s+1}\right).$$

To conclude, we need to show that $\mu_{s,d}(d)$ is equal to $\mu_{s+1,d}(d)$, that $\mu_{s,d}(j)-\mu_{s+1,d}(j+1)$ is equal to $\mu_{s+1,d}(j)$ for $0\le j\le d-1$, and that $\mu_{s,d}(j-1)+\mu_{s+1,d}(j-1)$ is equal to $\mu_{s+1,d}(j)$ for $2\le j\le d$. For the first equality, observe that both $\mu_{s,d}(d)$ and $\mu_{s+1,d}(d)$ are equal to 1. For the second and third equality, it follows from Pascal's rule. □

A.2 Proof of Lemma 9

Proof. If $x\ge 0$, then there exists $m>n$ and $(x_{n+1},\dots,x_m)\in\{0,\dots,p-1\}^{m-n}\subseteq\mathbb{Z}^{m-n}$ such that $x=\sum_{i\in[m]} x_i p^{i-1}$. By Lucas Theorem, we have that

$$\binom{\sum_{i\in[m]} x_i p^{i-1}}{p^{j-1}} = \binom{x_j}{1}\prod_{i\in[m]\setminus\{j\}}\binom{x_i}{0} = x_j \pmod p.$$

If $x<0$, then there exists $m>n$ and $(x'_1,\dots,x'_m)\in\{0,\dots,p-1\}^m\subseteq\mathbb{Z}^m$ such that $x=-\sum_{i\in[m]} x'_i p^{i-1}$. Observe that if $j=1$, then we have that

$$\binom{x}{1} = x = x_1 \pmod p.$$

Suppose that $j>1$. Let $k\in[m]$ be the smallest such that $x'_k\neq 0$. Then we have that

$$x=(p-x'_k)p^{k-1}+\sum_{i\in[k,n]}(p-1-x'_i)p^{i-1} \pmod{p^n}.$$

So we have that $x_j=-1-x'_j \pmod p$ if $k<j$ and $x_j=-x'_j \pmod p$ if $k\ge j$. Observe that

$$\binom{x}{p^{j-1}} = (-1)^{p^{j-1}}\binom{-x+p^{j-1}-1}{p^{j-1}} = -\binom{-x+p^{j-1}-1}{p^{j-1}} \pmod p$$

where the first equality follows by (2) and the second from the fact that $(-1)^{p^{j-1}} = (-1)^p = -1 \mod p$ since $j>1$. If $k<j$, then $\sum_{i\in[k,j-1]} x'_i p^{i-1}-1\in\{0,\dots,p^{j-1}-1\}$ and we have that

$$-\binom{-x+p^{j-1}-1}{p^{j-1}} = -\binom{(\sum_{i\in[k,j-1]} x'_i p^{i-1}-1)+(x'_j+1)p^{j-1}+\sum_{i\in[j+1,m]} x'_i p^{i-1}}{p^{j-1}}$$
$$= -\binom{(x'_j+1)}{1} = -x'_j-1 = x_j \pmod p.$$

If $k\ge j$, then $\sum_{i\in[k,j]} x'_i p^{i-1} = x'_j p^{j-1}$ and we have that

$$-\binom{-x+p^{j-1}-1}{p^{j-1}} = -\binom{(p^{j-1}-1)+x'_j p^{j-1}+\sum_{i\in[j+1,m]} x'_i p^{i-1}}{p^{j-1}}.$$

that is equal to $-\binom{x'_j}{1} = -x'_j = x_j \pmod p$. □