Cryptogr. Commun. (2015) 7:297–315
DOI 10.1007/s12095-014-0120-7

Characterization of robust immune symmetric boolean functions

Yuan Li

Received: 27 January 2013 / Accepted: 17 November 2014 / Published online: 30 November 2014

Abstract Fix a field $\mathbb{F}$. The algebraic immunity over $\mathbb{F}$ of boolean function $f : \{0,1\}^n \to \{0,1\}$ is defined as the minimal degree of a nontrivial (multilinear) polynomial $g(x) \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f(x)$ is a constant (either 0 or 1) for all $x \in \{0,1\}^n$ satisfying $g(x) = 0$. Function f is called k *robust immune* if the algebraic immunity of f is always not less than k no matter how one changes the value of $f(x)$ for $k \leq |x| \leq n-k$. For any field $\mathbb{F}$, any integers $n, k \geq 0$, we characterize all k robust immune symmetric boolean functions in n variables. The proof is based on a known symmetrization technique and constructing a partition of nonnegative integers satisfying certain (in)equalities about p-adic distance, where p is the characteristic of the field $\mathbb{F}$.

Keywords Algebraic immunity · Symmetric boolean functions · Characterization

Mathematics Subject Classification (2010) 06E30 · 94A60 · 94C10

1 Introduction

In cryptography community, algebraic immunity (over $\mathbb{F}_2$) is proposed as a criteria for boolean functions used in some stream ciphers to resist *algebraic attacks* [6]. In order to resist algebraic attacks (as well as many others), there are a lot of constructions aiming to achieve high algebraic immunity, high nonlinearity, balancedness, and so on [4, 5, 12, 15].

Symmetric boolean functions are those whose output is invariant under permutations of inputs. Regardless of its application in stream cipher, symmetric boolean functions are particularly well studied due to its relatively simple structure. It turns out all symmetric boolean functions with maximum algebraic immunity $\lceil n/2 \rceil$ can be completely characterized, cumulated along a line of research [2, 10, 11, 13, 14, 16], etc.

Y. Li (✉)
University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA
e-mail: yuanli@cs.uchicago.edu

In computational complexity, algebraic immunity (the same definition under different names!) also attracts some attention. Namely, (one-sided) *immunity* of f is defined as the minimal degree of a nontrivial polynomial g such that $f(x) = 0 \Rightarrow g(x) = 0$; immunity over $\mathbb{F}_p$ is also called *weak mod-p degree*. In circuit complexity, roughly speaking, lower bound on the algebraic immunity will imply circuit lower bound under various models [3, 7–9]. In proof complexity, immunity plus some expanding property implies degree lower bounds for Polynomial Calculus [1].

This work is motivated by the goal to characterize all symmetric boolean functions with *any* given algebraic immunity (not only maximum). To make the problem easier, we propose the definition of *k robust immune* (which is stronger than algebraic immunity), and end up with a complete characterization of k robust immune symmetric boolean function for any k over any field $\mathbb{F}$. The the first ingredient is a known symmetrization technique which has been successfully applied to understand algebraic immunity of *symmetric* Boolean functions. The main technical part is a construction of the (unique) partition of nonnegative integers which satisfies certain p-adic distance (in)equalities, which will imply a complete list of robust immune symmetric boolean functions.

2 Main result

Definition 1 Let $\mathbb{F}$ be a field, and $f : \{0, 1\}^n \to \{0, 1\}$ be a boolean function. The *algebraic immunity* of f over field $\mathbb{F}$ is defined as the minimal degree of a nontrivial[1] polynomial $g \in \mathbb{F}[x_1, \ldots, x_n]$, such that f becomes a constant when restricting to the zeros of g, i.e., there exists some $c \in \{0, 1\}$ such that $g(x) = 0 \Rightarrow f(x) = c$.

In cryptography community, algebraic immunity usually refers to that over $\mathbb{F}_2$, and can also be defined as the minimal $\mathbb{F}_2$-degree of some boolean function g such that $fg = 0$[2] or $(1 - f)g = 0$. If $fg = 0$, then g is called an *annihilator* of f (over boolean cube). In words, algebraic immunity of f is the smallest degree of some nonzero annihilator of either f or $1 - f$.

Definition 2 Boolean function $f : \{0, 1\}^n \to \{0, 1\}$ is called k robust immune over field $\mathbb{F}$ if the algebraic immunity of f over $\mathbb{F}$ is always not less than k no matter how one changes the values of $f(x)$ with $k \le |x| \le n - k$, where $|x| := x_1 + \ldots + x_n$ is the *weight* of x.

The definition of k robust immune looks a bit artificial. However, the reason why we allow changing values of $f(x)$ for $k \le |x| \le n - k$ instead of $k' \le |x| \le n - k'$ for some other k' is because $k' = k$ is the largest possible integer to take. Another reason we propose this definition is because we are able to characterize all k robust immune symmetric boolean functions, while the goal keeping in mind is to give such a characterization for all symmetric boolean functions with any given algebraic immunity.

Our main result is the following characterization of all k robust immune symmetric boolean functions for any given k over any field $\mathbb{F}$. For convenience, if $f : \{0, 1\}^n \to \{0, 1\}$ is symmetric, let $v_f : \{0, 1, \ldots, n\} \to \{0, 1\}$ be its *value vector*, that is, $f(x) = v_f(|x|)$.

[1] By *nontrivial*, we mean there exists some $x \in \{0, 1\}^n$ such that $g(x) = 0$.

[2] $fg = 0$ should be understood semantically, i.e., for every $x \in \{0, 1\}^n$, $f(x)g(x) = 0$; alternatively, $fg = 0$ could be understood as multiplication of polynomials over the quotient ring $F[x_1, \ldots, x_n]/(x_1^2 = x_1, \ldots, x_n^2 = x_n)$.

Theorem 1 *For any field $\mathbb{F}$, any integer $t \geq 0$, there exists a partition $\mathcal{P} = \mathcal{P}(\mathbb{F}, t)$ of nonnegative integers such that, for any k, symmetric boolean function $f : \{0,1\}^{2k+t-1} \to \{0,1\}$ is k robust immune if and only if*

$$v_f(k-1-i) = 1 - v_f(k+t+j) \tag{1}$$

for any $0 \leq i, j \leq k-1$ belonging to the same set in partition $\mathcal{P}$.

Remark 1 The partition $\mathcal{P} = \mathcal{P}(\mathbb{F}, t)$ will be defined explicitly in the following sequel, and $\mathcal{P}$ only depends on t and the *characteristic* of the field $\mathbb{F}$, which follows from the following linear algebra argument. Function f has no degree $\leq d$ annhilator if and only if some matrix of size $\binom{n}{\leq d} \times |f^{-1}(1)|$ has rank $\binom{n}{\leq d}$, which is a $\{0,1\}$-matrix[3]. It is clear that the rank of the $\{0,1\}$-matrix does not change over any field extension.

Remark 2 It is known that the algebraic immunity of any n-variable boolean function is upper bounded by $\lceil n/2 \rceil$, which is not difficult to see by a dimension argument. When $t = 0$, f is an odd-variable symmetric boolean functions with maximum algebraic immunity; and when $t = 1$, f is an even-variable symmetric boolean function with maximum algebraic immunity.[4] For the case $\mathbb{F} = \mathbb{F}_2$ and $t = 0, 1$, our theorem is implicitly known [11, 16]. For general field $\mathbb{F}$ and general t, our result is a nontrivial generalization.

3 Overview of the proof

The proof follows from a crucial symmetrization technique in [10] and the calculation of a determinant over the field $\mathbb{F}_p$. It turns out the symmetric boolean function is k robust immune if and only if some corresponding matrices have full rank, that is, the determinant is nonzero. Over the field $\mathbb{F}_p$, in order to prove the determinant is nonzero, the calculation involves a lot of *p-adic distance* estimates.

The following lemma says in order to prove symmetric boolean function f has no nonzero annihilator of certain degree, it suffices to consider the semi-symmetric annihilators up to that degree. The crucial lemma is proved by Liu and Feng in [10] for $\mathbb{F} = \mathbb{F}_2$, and observed in [3] that it works for any field.

Lemma 1 [10] *Let $\mathbb{F}$ be a field, and $f : \{0,1\}^n \to \{0,1\}$ be a symmetric boolean function. Then f has a lowest degree annihilator g of the following form,*

$$g = \prod_{i=1}^{l} (x_{2i-1} - x_{2i}) g',$$

where g' is a symmetric function in variables $x_{2l+1}, \ldots, x_n$.

For convenience, let us introduce the following notation $\psi_k : \mathbb{Z}_{\geq 0} \to \mathbb{F}^k$, where

$$\psi_k(x) = \left(\binom{x}{0}, \binom{x}{1}, \ldots, \binom{x}{k-1} \right) \in \mathbb{F}^k,$$

[3] The rows are indexed by subsets of $[n]$ of size $\leq d$, the columns are indexed by points $x \in \{0,1\}^n$ such that $f(x) = 1$, and the entry (S, x) is exactly $\prod_{i \in S} x_i$.

[4] The converse is not true, that is, there are $2k$-variable symmetric boolean functions with maximum algebraic immunity k which are *not* k robust immune. However, they are "close" to some k robust immune functions.

where $\binom{x}{i} = \underbrace{1+1+\ldots+1}_{\binom{x}{i} \text{ times}}$. In other words, $\binom{x}{i} = \binom{x}{i} \pmod p$ over field $\mathbb{F}_p$. The following proposition is an immediate consequence of Lemma 1.

Proposition 1 *Let $f : \{0,1\}^n \to \{0,1\}$ be a symmetric boolean function, and $v_f : \{0,1,\ldots,n\} \to \{0,1\}$ be its corresponding value vector. Function f is k robust immune if and only if, for any $0 \le l \le k-1$, both*

$$\{\psi_{k-l}(i-l) : i \in [l, k-1] \cup [n-k+1, n-l] \text{ and } v_f(i) = 0\} \tag{2}$$

and

$$\{\psi_{k-l}(i-l) : i \in [l, k-1] \cup [n-k+1, n-l] \text{ and } v_f(i) = 1\} \tag{3}$$

are bases of $\mathbb{F}^{k-l}$.

Proof By the definition of k robust immune, for symmetric boolean function f, it suffices to prove f_0 has no annihilator of degree $< k$, and $1 - f_1$ has no annihilator of degree $< k$, where

$$v_{f_0}(x) = \begin{cases} v_f(x) & x \in [0, k-1] \cup [n-k+1, n] \\ 0 & \text{otherwise} \end{cases}$$

and

$$v_{f_1}(x) = \begin{cases} v_f(x) & x \in [0, k-1] \cup [n-k+1, n] \\ 1 & \text{otherwise.} \end{cases}$$

By Lemma 1, f_0 (the argument for f_1 is similar) has no annihilator of degree $< k$ if and only if it has no annihilator of the form $g = \prod_{i=1}^{l}(x_{2i-1} - x_{2i})g'$, where g' is a symmetric function in $x_{2l+1}, \ldots, x_n$ of degree $< k - l$. Fix some $0 \le l \le k-1$. $f_0 g = 0 \Leftrightarrow f_0 \prod_{i=1}^{l}(x_{2i-1} - x_{2i})g' = 0$, which is equivalent to $f_0' g' = 0$, where

$$f_0' = f_0|_{x_1 = x_3 = \ldots = x_{2l-1} = 1, x_2 = x_4 = \ldots = x_{2l} = 0}.$$

It is easily checked that $v_{f_0'} = (v_{f_0}(l), v_{f_0}(l+1), \ldots, v_{f_0}(n-l))$. Note that both f_0' and g' are symmetric, and $\deg(g') < k - l$. Thus we may write

$$g' = a_0 e_0 + \ldots + a_{k-l-1} e_{k-l-1},$$

where e_i is the *elementary symmetric polynomial* of degree i, which takes value $\binom{x}{i}$ at any point with weight i. The condition $f_0' g' = 0$ is equivalent to $g'(x) = 0$ for all $v_{f_0'}(x) = 1$, i.e., $a_0\binom{x}{0} + a_1\binom{x}{1} + \ldots + a_{k-l-1}\binom{x}{k-l-1} = 0$. Therefore, such g' exists if and only if there exists a nonzero $a \in \mathbb{F}^{k-l}$ such that $a^T \psi_{k-l}(x) = 0$ for all $v_{f_0'}(x) = v_f(x+l) = 1$, that is, $\{\psi_{k-l}(i-l) : i \in [l, k-1] \cup [n-k+1, n-l] \text{ and } v_f(i) = 1\}$ has rank $< k - l$. □

Remark 3 From the above proposition, we can see if symmetric f is k robust immune, then $v_f(i) = 1 - v_f(n-i)$ for $0 \le i \le k-1$, and $f|_{x_1=1, x_2=0}$ is $k-1$ robust immune.

Next step is to notice $\psi_k(x_0), \psi_k(x_1), \ldots, \psi_k(x_{k-1})$ has full rank if and only if the determinant is nonzero (over the field $\mathbb{F}$), where the determinant turns out to have the following simple form [3][5]

$$\det(\psi_k(x_0), \psi_k(x_1), \ldots, \psi_k(x_{k-1})) = \prod_{0 \le i < j \le k-1} \frac{x_j - x_i}{j - i}. \tag{4}$$

[5]The computation consists of some simple manipulations reducing to Vandermonde matrix.

Over the the field $\mathbb{F}$ with characteristic 0, the above determinant is always nonzero for distinct $x_0, \ldots, x_{k-1}$, which implies $\mathcal{P}(\mathbb{F}, t) = \{\{0\}, \{1\}, \{2\}, \ldots\}$ for any $t \geq 0$; over field with characteristic p, the determinant is nonzero if and only if

$$\sum_{0 \leq i < j \leq k-1} \mathrm{ord}_p(x_j - x_i) = \sum_{0 \leq i < j \leq k-1} \mathrm{ord}_p(j - i), \tag{5}$$

where $\mathrm{ord}_p(x)$ is the *p-adic order* of x, that is, the maximum integer m such that p^m divides x. *From now on, we will assume $\mathbb{F} = \mathbb{F}_p$ for some prime p.*

Combining (4) with Proposition 1, we have the following lemma, which says if the partition $\mathcal{P}$ satisfies certain condition, then the functions in Theorem 1 are k robust immune.

Lemma 2 (**Sufficiency**) *Fix some integer $t \geq 0$ and $k > 0$. Let $\mathcal{P}$ be a partition of $\{0, \ldots, k-1\}$, i.e., $\mathcal{P} = \{I_0, I_1, \ldots\}$, where $\dot{\cup}_{i \geq 0} I_i = \{0, \ldots, k-1\}$. If for all $I \in \mathcal{P}$, we have*

$$\sum_{x \in I \text{ and } x < y} \mathrm{ord}_p(y - x) = \sum_{x \in I \text{ and } x < y} \mathrm{ord}_p(y + x + t + 1) \tag{6}$$

for all $0 \leq y \leq k-1$ with $y \notin I$, then all symmetric boolean functions satisfying (1) are k robust immune.

Proof By Proposition 1, it suffices to prove that for all l, both (2) and (3) are bases of $\mathbb{F}^{k-l}$. With loss of generality, assume $l = 0$, and we shall prove (2) is a basis of $\mathbb{F}^k$.

By condition (1), we know that, there exists index set S such that

$$\{k - 1 - i : v_f(i) = 0 \text{ and } i \in [0, k-1]\} = \bigcup_{i \in S} I_i,$$

and

$$\{i - k - t : v_f(i) = 0 \text{ and } i \in [k + t, 2k + t - 1]\} = \bigcup_{i \notin S} I_i,$$

where $\mathcal{P} = \dot{\cup}_i I_i$. By (5), it suffices to prove

$$\sum_{0 \leq i < j \leq k-1} \mathrm{ord}_p(j - i) = \sum_{0 \leq i < j \leq k-1} \mathrm{ord}_p(x_j - x_i),$$

where x_j is either $k - 1 - j$ or $k + t + j$, depending on whether $j \in \cup_{i \in S} I_i$ or not.

$$\begin{aligned}
&\sum_{0 \leq i < j \leq k-1} \mathrm{ord}_p(x_j - x_i) \\
&= \sum_{\substack{i < j \\ i,j \in S \text{ or } i,j \notin S}} \mathrm{ord}_p(j - i) + \sum_{\substack{i < j \\ i \in S, j \notin S \text{ or } i \notin S, j \in S}} \mathrm{ord}_p(j + i + t + 1) \\
&= \sum_{\substack{i < j \\ i,j \in S \text{ or } i,j \notin S}} \mathrm{ord}_p(j - i) + \sum_{\substack{i < j \\ i \in S, j \notin S \text{ or } i \notin S, j \in S}} \mathrm{ord}_p(j - i) \\
&= \sum_{0 \leq i < j \leq k-1} \mathrm{ord}_p(j - i),
\end{aligned}$$

where the second last step follows from our condition (6). □

Lemma 3 (Necessity) *Fix some integer $t \geq 0$ and $k > 0$. Let $\mathcal{P}$ be a partition of $\{0, \ldots, k-1\}$ satisfying (6) in Lemma 2. If for any $y \in I \in \mathcal{P}$ with $\{x \in I : x < y\}$ nonempty,*

$$\sum_{x \in I \text{ and } x<y} \mathrm{ord}_p(y-x) < \sum_{x \in I \text{ and } x<y} \mathrm{ord}_p(y+x+t+1), \tag{7}$$

then all k robust immune symmetric boolean functions satisfy (1).

Proof Let $\mathcal{P}$ be a partition of $\{0, 1, \ldots, k-1\}$ satisfying the conditions in this lemma. Assume for contradiction that there exists some k robust immune symmetric boolean function which does *not* satisfy (1).

Let $0 \leq i < j \leq k-1$ be some pair which violates (1) with *minimum* j. Let $l = k-1-j$, and we shall prove

$$\{\psi_{k-l}(i-l) : i \in [l, k-1] \cup [n-k+1, n-l] \text{ and } v_f(i) = 0\} \tag{8}$$

is not a basis of $\mathbb{F}^{k-l}$, which would be a contradiction to Proposition 1.

Let $\mathcal{P} \cap \{0, 1, \ldots, k-l-1\} = \{I_0, I_1, \ldots, I_m\}$, which is the partition of $\{0, 1, \ldots, k-l-1\}$ induced by $\mathcal{P}$. Without loss of generality, assume $j \in I_m$. Then the set (8) is exactly the union of

$$\{\psi_{k-l}(k-1-x-l) : x \in I_0\} \text{ or } \{\psi_{k-l}(k+t+x-l) : x \in I_0\}$$
$$\{\psi_{k-l}(k-1-x-l) : x \in I_1\} \text{ or } \{\psi_{k-l}(k+t+x-l) : x \in I_1\}$$
$$\vdots$$
$$\{\psi_{k-l}(k-1-x-l) : x \in I_{m-1}\} \text{ or } \{\psi_{k-l}(k+t+x-l) : x \in I_{m-1}\}$$
$$\{\psi_{k-l}(k-1-x-l) : x \in I_m \setminus \{j\}\} \cup \{\psi_{k-l}(k+t+j-l)\}$$
$$\text{or } \{\psi_{k-l}(k+t+x-l) : x \in I_m \setminus \{j\}\} \cup \{\psi_{k-l}(k-1-j-l)\}.$$

Following the same calculation as we did in Lemma 2, we claim that the order of the determinant is exactly

$$\sum_{x \in I_m \text{ and } x<y} \mathrm{ord}_p(y+x+t+1) - \sum_{x \in I_m \text{ and } x<y} \mathrm{ord}_p(y-x),$$

which is greater than 0 by our condition in the lemma, and thus the determinant over $\mathbb{F}_p$ is zero, and therefore (8) is not a basis. □

Given field $\mathbb{F}$, integer t, k, assuming there exists a partition $\mathcal{P}$ of $\{0, 1, \ldots, k-1\}$ satisfying (6) and (7), then by Lemma 2 and Lemma 3, we will obtain all k robust immune symmetric boolean functions in $2k+t-1$ variables. It remains to prove the existence of such partitions, and we will construct $\mathcal{P}$ inductively on t. An interesting feature, which in fact follows from (6) and (7), is that $\mathcal{P}$ does not depend on k, that is to say, $\mathcal{P}(\mathbb{F}, t, k)$ and $\mathcal{P}(\mathbb{F}, t, k+1)$ induce the same equivalence relation on $\{0, 1, \ldots, k-1\}$. Let us summarize the conditions we need on $\mathcal{P}(\mathbb{F}_p, t)$, which is our main technical lemma.

Lemma 4 (Main technical lemma) *For any prime p, and any integer $t \geq 0$, there exists a partition $\mathcal{P} = \mathcal{P}(\mathbb{F}_p, t)$ of nonnegative integers satisfying the followings.*

– *(Soundness) For all $I \in \mathcal{P}$, $y \notin I$, we have*

$$\sum_{x \in I \text{ and } x<y} \mathrm{ord}_p(y-x) = \sum_{x \in I \text{ and } x<y} \mathrm{ord}_p(y+x+t+1). \tag{9}$$

– *(Completeness) For any $y \in I \in \mathcal{P}$ with $\{x \in I : x < y\}$ nonempty,*

$$\sum_{x \in I \text{ and } x<y} \operatorname{ord}_p(y-x) < \sum_{x \in I \text{ and } x<y} \operatorname{ord}_p(y+x+t+1). \tag{10}$$

Putting everything together, it is easy to see Lemma 4 together with Lemma 2 and Lemma 2 implies our main theorem. All the remaining pages are devoted to the constructive proof of Lemma 4, which is a bit tedious. It would be interesting to find a simpler proof of Lemma 4, probably an existential proof.

4 Proof for the case char($\mathbb{F}$) = 2

In this section, we will prove Lemma 4 for $\mathbb{F} = \mathbb{F}_2$.

Notations We are introducing some handy notations, which are nonstandard but will be convenient and intuitive for the following proofs. For $p = 2$ (or any prime $p \geq 2$), integer $x \geq 0$ has a unique p-adic expansion[6]

$$x = (x_0, x_1, x_2, \ldots)_2,$$

where $x = \sum_{i \geq 0} x_i 2^i$. When there is no ambiguity, we will drop the subscript 2 . A *pattern*, either denoted by an p-adic expansion or Greek alphabets α, β, is *subset* of $\mathbb{Z}_{\geq 0}$ descried by p-adic expansion by the following rules.

– Character $*$ denotes any 01-string of *arbitrary* length, that is, pattern $(*)$ is exactly $\mathbb{Z}_{\geq 0}$.
– Character ? denotes a single bit, i.e., either 0 or 1. For example, $(?, 0, *)$ denotes the set of nonnegative integers congruent to 0, 1 mod 4.
– An integer superscript i means repeating i times. For example, $(0^i, *)$ denotes the set of nonnegative integers which are multiples of 2^i.
– If α is a pattern, it can be put at the end of p-adic expansion to define a new pattern, like $(0, 0, \alpha)$, which is the set of integers $4x$, $x \in \alpha$.
– Since patterns are sets, set operations can be applied. For example, $\alpha \cap [0, y]$ is $\{x \in \alpha : x \leq y\}$.

We are ready to define partition $\mathcal{P}(\mathbb{F}_2, t)$. Within this section, we may simply write $\mathcal{P}(\mathbb{F}_2, t)$ as $\mathcal{P}(t)$.

Definition 3 Let $\mathcal{P}(0) = \{(*)\}$ and $\mathcal{P}(1) = \{(1^i, 0, *) : i = 0, 1, \ldots\}$. For integer $t \geq 1$,

$$\mathcal{P}(2t) = \{(?, \alpha) : \alpha \in \mathcal{P}(t)\}.$$

For odd integer $t \geq 1$,

$$\mathcal{P}(2t+1) = \{(0, 0, \alpha) : (0, \alpha) \in \mathcal{P}(t)\} \cup \{(1, ?, \alpha), (0, 1, \alpha) : (1, \alpha) \in \mathcal{P}(t)\}.$$

For odd integer $t \geq 1$ and $e \geq 2$,

$$\mathcal{P}(2^e t + 1) = \{(1^e, \alpha) : \alpha \in \mathcal{P}(t+1)\} \cup \{(1^i, 0, ?^{e-1-i}, \alpha) : \alpha \in \mathcal{P}(t), 0 \leq i \leq e-1\}.$$

[6]Or equivalently, embed $\mathbb{Z}_{\geq 0}$ into the ring of p-adic integers $\mathbb{Z}_p$, which is a formal series $x = \sum_{i \geq 0} x_i p^i$.

It is not difficult to see $\mathcal{P}(t)$ is well-defined, that is, it is a partition of $\mathbb{Z}_{\geq 0}$. To make sure the readers understand our definition of $\mathcal{P}(t)$, let us restate the the definition in standard set notations.

$$\begin{aligned}
\mathcal{P}(0) &= \{\mathbb{Z}_{\geq 0}\}.\\
\mathcal{P}(1) &= \{2^{r+1}\mathbb{Z}_{\geq 0} + 2^r - 1 : r = 0, 1, \ldots\}.\\
\mathcal{P}(2t) &= \{2I \cup (2I+1) : I \in \mathcal{P}(t)\}.\\
\mathcal{P}(2t+1) &= \{2I : I \in \mathcal{P}(t) \text{ and } I \subseteq 2\mathbb{Z}_{\geq 0}\} \cup\\
&\quad \{2I, (2I+1) \cup (2I-1) : I \in \mathcal{P}(t) \text{ and } I \subseteq 2\mathbb{Z}_{\geq 0} + 1\}.\\
\mathcal{P}(2^e t + 1) &= \{2^e I + 2^e - 1 : I \in \mathcal{P}(t+1)\} \cup\\
&\quad \{\bigcup_{0 \leq j \leq 2^{e-1-i}-1} 2^e I + 2^{i+1} j + 2^i - 1 : I \in \mathcal{P}(t), 0 \leq i \leq e-1\}.
\end{aligned}$$

In the following subsections, we will prove Lemma 4 for $p = 2$ by induction on t. According to our definition of $\mathcal{P}(t)$, the proof consists of 5 cases, that is, $0, 1, 2t, 2t+1, 2^e t + 1$.

4.1 $\mathcal{P}(\mathbb{F}_2, 0)$

Recall that $\mathcal{P}(0) = \{\mathbb{Z}_{\geq 0}\}$. Soundness is trivially true. For completeness, we need to prove

$$\sum_{0 \leq x < y} \mathrm{ord}_2(y - x) < \sum_{0 \leq x < y} \mathrm{ord}_2(y + x + 1) \tag{11}$$

for any $x > 0$, which is equivalent to $\mathrm{ord}_2(y!) < \mathrm{ord}_2((2y)!/y!)$, which is true because $\binom{2y}{y} \equiv 0 \pmod 2$ for any $y > 0$. We leave it as an exercise for readers, and (11) will be used again.

4.2 $\mathcal{P}(\mathbb{F}_2, 1)$

Recall that $\mathcal{P}(1) = \{(1^i, 0, *) : i = 0, 1, \ldots\}$. For soundness, let $x \in (1^i, 0, *)$ and $y \in (1^j, 0, *)$, where $i \neq j$. It is easily checked that $\mathrm{ord}_2(x - y) = \mathrm{ord}_2(x + y + 2) = \min(i, j)$, which proves the soundness.

For completeness, let $y \in I = (1^i, 0, *)$ with $I \cap [0, y-1]$ nonempty, and we shall prove

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_2(y - x) < \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_2(y + x + 2).$$

Let $y = (y_0 = 1, \ldots, y_{i-1} = 1, y_i = 0, y_{\geq i+1})$, where $y_{\geq i+1}$ denotes the integer $(y_{i+1}, y_{i+2}, \ldots)$, that is, $\sum_{j \geq 0} 2^j y_{i+j+1}$. Adopt the same notation for x. It is easily checked that

$$\mathrm{ord}_2(y - x) = i + 1 + \mathrm{ord}_2(y_{\geq i+1} - x_{\geq i+1})$$

and

$$\mathrm{ord}_2(y + x + 2) = i + 1 + \mathrm{ord}_2(y_{\geq i+1} + x_{\geq i+1} + 1).$$

Thus, it is equivalent to prove[7]

$$\sum_{0\le x_{\ge i+1}<y_{\ge i+1}} \mathrm{ord}_2(y_{\ge i+1}-x_{\ge i+1}) < \sum_{0\le x_{\ge i+1}<y_{\ge i+1}} \mathrm{ord}_2(y_{\ge i+1}+x_{\ge i+1}+1)$$

for any $y_{\ge i+1} > 0$ (by assumption $\{x \in I : x < y\}$ is nonempty), which is exactly (11).

4.3 $\mathcal{P}(\mathbb{F}_2, 2t)$

By definition, $\mathcal{P}(2t) = \{(?, \alpha) : \alpha \in \mathcal{P}(t)\}$.

Soundness Need to prove for any $y \notin I \in \mathcal{P}(2t)$

$$\sum_{x\in I\cap[0,y-1]} \mathrm{ord}_2(y-x) = \sum_{x\in I\cap[0,y-1]} \mathrm{ord}_2(y+x+2t+1). \tag{12}$$

Let $I = (?, \alpha)$, where $\alpha \in \mathcal{P}(t)$. Let $y = (y_0, y_1, \ldots)$, where $y_{\ge 1} \notin \alpha$ by assumption $y \notin I$. The left hand side of (12) is

$$\begin{aligned}
&\sum_{x\in I\cap[0,y-1]} \mathrm{ord}_2(y-x)\\
&= \sum_{x_{\ge 1}\cap[0,y_{\ge 1}-1]} \mathrm{ord}_2((y_0, y_{\ge 1}) - (y_0, x_{\ge 1}))\\
&= |\alpha \cap [0, y_{\ge 1}-1]| + \sum_{x_{\ge 1}\cap[0,y_{\ge 1}-1]} \mathrm{ord}_2(y_{\ge 1}-x_{\ge 1}).
\end{aligned}$$

The right hand side of (12) is

$$\begin{aligned}
&\sum_{x\in I\cap[0,y-1]} \mathrm{ord}_2(y+x+2t+1)\\
&= \sum_{x_{\ge 1}\in\alpha\cap[0,y_{\ge 1}-1]} \mathrm{ord}_2((y_0, y_{\ge 1}) + (1-y_0, x_{\ge 1}) + (1, t))\\
&= |\alpha \cap [0, y_{\ge 1}-1]| + \sum_{x_{\ge 1}\in\alpha\cap[0,y_{\ge 1}-1]} \mathrm{ord}_2(y_{\ge 1}+x_{\ge 1}+t+1).
\end{aligned}$$

By induction hypothesis, $\mathcal{P}(t)$ is sound, and thus $\sum_{x_{\ge 1}} \mathrm{ord}_2(y_{\ge 1} + x_{\ge 1} + t + 1) = \sum_{x_{\ge 1}} \mathrm{ord}_2(y_{\ge 1} - x_{\ge 1})$, which proves (12).

Completeness We shall prove, for any $y \in I \in \mathcal{P}$ with $\{x \in I : x < y\}$ nonempty,

$$\sum_{x\in I\cap[0,y-1]} \mathrm{ord}_2(y-x) < \sum_{x\in I\cap[0,y-1]} \mathrm{ord}_2(y+x+t+1). \tag{13}$$

Let $I = (?, \alpha)$, where $\alpha \in \mathcal{P}(t)$. The left hand side of (13) is $|\alpha \cap [0, y_{\ge 1} - 1]| + \sum_{x_{\ge 1}<y_{\ge 1}} \mathrm{ord}_2(y_{\ge 1} - x_{\ge 1})$, while the right hand side is at least

$$|\alpha \cap [0, y_{\ge 1}-1]| + \sum_{x_{\ge 1}<y_{\ge 1}} \mathrm{ord}_2(y_{\ge 1}+x_{\ge 1}+t+1) + \delta_{y_0,1},$$

[7] In the following inequality, we could have written x instead of $x_{\ge i+1}$. We are denoting the variable by $x_{\ge i+1}$ for bit alignment.

where $\delta_{y_0,1} = 1$ if $y_0 = 1$, otherwise 0. If $\alpha \cap [0, y_{\geq 1} - 1]$ is nonempty, we have $\sum_{x_{\geq 1} < y_{\geq 1}} \mathrm{ord}_2(y_{\geq 1} + x_{\geq 1} + t + 1) > \sum_{x_{\geq 1} < y_{\geq 1}} \mathrm{ord}_2(y_{\geq 1} - x_{\geq 1})$ by the completeness of $\mathcal{P}(t)$, which implies (13); otherwise $y_0 = 1$, which also implies (13).

4.4 $\mathcal{P}(\mathbb{F}_2, 2t + 1)$, t odd

Recall the definition, $\mathcal{P}(2t+1) = \{(0, 0, \alpha) : (0, \alpha) \in \mathcal{P}(t)\} \cup \{(1, ?, \alpha), (0, 1, \alpha) : (1, \alpha) \in \mathcal{P}(t)\}$, where all patterns in $\mathcal{P}(t)$ are of the form $(0, \alpha)$ or $(1, \alpha)$ by definition.

Soundness We need to prove for any $y \notin I \in \mathcal{P}(2t + 1)$

$$\sum_{x \in I \text{ and } x < y} \mathrm{ord}_2(y - x) = \sum_{x \in I \text{ and } x < y} \mathrm{ord}_2(y + x + 2t + 2). \tag{14}$$

Let us prove by case analysis according to the patterns of y and I.

Case 1 $y \in (0, 0, \alpha)$ and $I = (1, ?, \beta)$, where $(0, \alpha), (1, \beta) \in \mathcal{P}(t)$. Both the left and right of (14) are 0.

Case 2 $y \in (0, 0, \alpha)$ and $I = (0, 1, \beta)$, where $(0, \alpha), (1, \beta) \in \mathcal{P}(t)$. The left of (14) is $|I \cap [0, y - 1]|$, and the right is $\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_2(y + x + 2t + 2) = \sum \mathrm{ord}((0, 0, y_{\geq 2}) + (0, 1, x_{\geq 2}) + (0, t + 1)) = |I \cap [0, y - 1]|$.

Case 3 $y \in (1, ?, \alpha)$ and $I = (0, 0, \beta)$, where $(1, \alpha), (0, \beta) \in \mathcal{P}(t)$. Both the left and right of (14) are 0.

Case 4 $y \in (1, ?, \alpha)$ and $I = (0, 1, \beta)$, where $(1, \alpha), (1, \beta) \in \mathcal{P}(t)$. Both the left and right of (14) are 0.

Case 5 $y \in (0, 1, \alpha)$ and $I = (0, 0, \beta)$, where $(1, \alpha), (0, \beta) \in \mathcal{P}(t)$. It is similar to Case 2.

Case 6 $y \in (0, 1, \alpha)$ and $I = (1, ?, \beta)$, where $(1, \alpha), (1, \beta) \in \mathcal{P}(t)$. Both the left and right of (14) are 0.

Case 7 $y \in (0, 0, \alpha)$ and $I = (0, 0, \beta)$, where $(0, \alpha), (0, \beta) \in \mathcal{P}(t)$ and $\alpha \neq \beta$. The left of (14) is

$$\begin{aligned} &\sum_{x_{\geq 1} \in (0,\alpha) \cap [0, y_{\geq 1} - 1]} \mathrm{ord}_2((0, y_{\geq 1}) - (0, x_{\geq 1})) \\ &= |(0, \alpha) \cap [0, y_{\geq 1} - 1]| + \sum_{x_{\geq 1} \in (0,\alpha) \cap [0, y_{\geq 1} - 1]} \mathrm{ord}_2(y_{\geq 1} - x_{\geq 1}), \end{aligned}$$

and the right of (14) is

$$\begin{aligned} &\sum_{x_{\geq 1} \in (0,\alpha) \cap [0, y_{\geq 1} - 1]} \mathrm{ord}_2((0, y_{\geq 1}) + (0, x_{\geq 1}) + (0, t + 1)) \\ &= |(0, \alpha) \cap [0, y_{\geq 1} - 1]| + \sum_{x_{\geq 1} \in (0,\alpha) \cap [0, y_{\geq 1} - 1]} \mathrm{ord}_2(y_{\geq 1} + x_{\geq 1} + t + 1). \end{aligned}$$

By induction hypothesis that $\mathcal{P}(t)$ is sound and $(0, \alpha) \in \mathcal{P}(t)$, we have $\sum \mathrm{ord}_2(y_{\geq 1} - x_{\geq 1}) = \sum \mathrm{ord}_2(y_{\geq 1} + x_{\geq 1} + t + 1)$, which implies (14).

Case 8 $y \in (1, ?, \alpha)$ and $I = (1, ?, \beta)$, where $(1, \alpha), (1, \beta) \in \mathcal{P}(t)$ and $\alpha \neq \beta$. It is not difficult to verify that the left of (14) is

$$2|\alpha \cap [0, y_{\geq 2} - 1]| + \sum_{x_{\geq 2} \in \alpha \cap [0, y_{\geq 2} - 1]} \mathrm{ord}_2((1, y_{\geq 2}) - (1, x_{\geq 2})),$$

and the right of (14) is

$$2|\alpha \cap [0, y_{\geq 2} - 1]| + \sum_{x_{\geq 2} \in \alpha \cap [0, y_{\geq 2} - 1]} \mathrm{ord}_2((1, y_{\geq 2}) + (1, x_{\geq 2}) + t + 1).$$

By the induction hypothesis that $\mathcal{P}(t)$ is sound, and $(1, y_{\geq 2}) \in (1, \alpha) \in \mathcal{P}(t)$, we have $\sum \mathrm{ord}_2((1, y_{\geq 2}) - (1, x_{\geq 2})) = \sum \mathrm{ord}_2((1, y_{\geq 2}) + (1, x_{\geq 2}) + t + 1)$, which implies (14).

Case 9 $y \in (0, 1, \alpha)$ and $I = (0, 1, \beta)$, where $(1, \alpha), (1, \beta) \in \mathcal{P}(t)$ and $\alpha \neq \beta$. The left of (14) is

$$|\beta \cap [0, y_{\geq 2}]| + \sum_{x_{\geq 2} \in \beta \cap [0, y_{\geq 2} - 1]} \mathrm{ord}_2((1, y_{\geq 2}) - (1, x_{\geq 2}))$$

and the right of (14) is

$$|\beta \cap [0, y_{\geq 2}]| + \sum_{x_{\geq 2} \in \beta \cap [0, y_{\geq 2} - 1]} \mathrm{ord}_2((1, y_{\geq 2}) + (1, x_{\geq 2}) + t + 1).$$

By the induction hypothesis, $\mathcal{P}(t)$ is sound, then for $(1, y_{\geq 2}) \in (1, \alpha) \in \mathcal{P}(t)$, $(1, \beta) \in \mathcal{P}(t)$, we have $\sum \mathrm{ord}_2((1, y_{\geq 2}) - (1, x_{\geq 2})) = \sum \mathrm{ord}_2((1, y_{\geq 2}) + (1, x_{\geq 2}) + t + 1)$,which proves (14).

Completeness We will prove the completeness of $\mathcal{P}(2t + 1)$, which amounts to, for any $y \in I \in \mathcal{P}(2t + 1)$ with $\{x \in I : x < y\}$ nonempty,

$$\sum_{x \in I \text{ and } x < y} \mathrm{ord}_2(y - x) < \sum_{x \in I \text{ and } x < y} \mathrm{ord}_2(y + x + 2t + 2). \tag{15}$$

Case 1 $y \in I = (0, 0, \alpha)$, where $y_{\geq 1} \in (0, \alpha) \in \mathcal{P}(t)$. The left of (15) is

$$|I \cap [0, y - 1]| + \sum_{x_{\geq 1} \in (0, \alpha) \cap [0, y_{\geq 1} - 1]} \mathrm{ord}_2(y_{\geq 1} - x_{\geq 1}),$$

and the right of (15) is

$$|I \cap [0, y - 1]| + \sum_{x_{\geq 1} \in (0, \alpha) \cap [0, y_{\geq 1} - 1]} \mathrm{ord}_2(y_{\geq 1} + x_{\geq 1} + t + 1).$$

Observe that $y_{\geq 1} \in (0, \alpha) \in \mathcal{P}(t)$ and $(0, \alpha) \cap [0, y_{\geq 1} - 1]$ is nonempty. By the completeness of $\mathcal{P}(t)$, we have $\sum \mathrm{ord}_2(y_{\geq 1} - x_{\geq 1}) < \sum \mathrm{ord}_2(y_{\geq 1} + x_{\geq 1} + t + 1)$, which implies (15).

Case 2 $y \in I = (1, ?, \alpha)$, where $(1, y_{\geq 2}) \in (1, \alpha) \in \mathcal{P}(t)$. It is not difficult to verify the left hand side of (15) is

$$2|\alpha \cap [0, y_{\geq 2} - 1]| + \delta_{y_1, 1} + \sum_{x_{\geq 2} \in \alpha \cap [0, y_{\geq 2} - 1]} \mathrm{ord}_2((1, y_{\geq 2}) - (1, x_{\geq 2})),$$

while the right of (15) is at least

$$2|\alpha \cap [0, y_{\geq 2} - 1]| + 2\delta_{y_1,1} + \sum_{x_{\geq 2} \in \alpha \cap [0, y_{\geq 2} - 1]} \mathrm{ord}_2((1, y_{\geq 2}) + (1, x_{\geq 2}) + t + 1).$$

Given $(1, ?, \alpha) \cap [0, y - 1]$ nonempty, we either have $(1, \alpha) \cap [0, y_{\geq 2} - 1]$ nonempty, or $y_1 = 1$. In the former case, $\sum_{x_{\geq 2}} \mathrm{ord}_2((1, y_{\geq 2}) - (1, x_{\geq 2})) < \sum_{x_{\geq 2}} \mathrm{ord}_2((1, y_{\geq 2}) + (1, x_{\geq 2}) + t + 1)$ by the completeness of $\mathcal{P}(t)$, which implies (15); in the latter case, (15) is also true.

Case 3 $y \in I = (0, 1, \alpha)$, where $(1, y_{\geq 2}) \in (1, \alpha) \in \mathcal{P}(t)$. The left of (15) is

$$|(1, \alpha) \cap [0, y_{\geq 1} - 1]| + \sum_{x_{\geq 1} \in (1,\alpha) \cap [0, y_{\geq 1} - 1]} (y_{\geq 1} - x_{\geq 1}),$$

while the right of (15) is

$$|(1, \alpha) \cap [0, y_{\geq 1} - 1]| + \sum_{x_{\geq 1} \in (1,\alpha) \cap [0, y_{\geq 1} - 1]} (y_{\geq 1} + x_{\geq 1} + t + 1).$$

From the completeness of $\mathcal{P}(t)$, we have $\sum(y_{\geq 1} - x_{\geq 1}) < \sum(y_{\geq 1} + x_{\geq 1} + t + 1)$, which implies (15).

4.5 $\mathcal{P}(\mathbb{F}_2, 2^e t + 1)$, t odd, $e \geq 2$

Recall the definition, for $e \geq 2$ and odd t,

$$\mathcal{P}(2^e t + 1) = \{(1^e, \alpha) : \alpha \in \mathcal{P}(t + 1)\} \cup \{(1^i, 0, ?^{e-1-i}, \alpha) : \alpha \in \mathcal{P}(t), 0 \leq i \leq e - 1\}.$$

Soundness We need to show for any $y \notin I \in \mathcal{P}(2^e t + 1)$

$$\sum_{x \in I \text{ and } x < y} \mathrm{ord}_2(y - x) = \sum_{x \in I \text{ and } x < y} \mathrm{ord}_2(y + x + 2^e t + 2). \tag{16}$$

Again, it will be case analysis according to the definition.

Case 1 $y \in (1^e, \alpha)$ and $I = (1^i, 0, ?^{e-1-i}, \beta)$, where $\alpha \in \mathcal{P}(t + 1)$ and $\beta \in \mathcal{P}(t)$. The left of (16) is $i|\beta \cap [0, y_{\geq e} - 1]|$, and the right of (16) is

$$\sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e} - 1]} \mathrm{ord}_2((1^e, y_{\geq e}) + (1^i, 0, ?^{e-1-i}, x_{\geq e}) + (0, 1, 0^{e-2}, t)),$$

which is also $i|\beta \cap [0, y_{\geq e} - 1]|$. Thus, (16) is true.

Case 2 $y \in (1^i, 0, ?^{e-1-i}, \alpha)$ and $I = (1^e, \alpha)$. Similar with Case 1, both sides of (16) is $i|\beta \cap [0, y_{\geq e} - 1]|$.

Case 3 $y \in (1^e, \alpha)$ and $I = (1^e, \beta)$, where $\alpha, \beta \in \mathcal{P}(t+1)$ and $\alpha \neq \beta$. The left of (16) is $e|\alpha \cap [0, y_{\geq e} - 1]| + \sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} - x_{\geq e})$, while the right of (16) is

$$\begin{aligned}
&\sum_{x \in I \text{ and } x<y} \mathrm{ord}_2(y + x + 2^e t + 2) \\
&= \sum_{x \in I \text{ and } x<y} \mathrm{ord}_2((1^e, y_{\geq e}) + (1^e, x_{\geq e}) + (0, 1, 0^{e-2}, t)) \\
&= e|\alpha \cap [0, y_{\geq e} - 1]| + \sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} + x_{\geq e} + t + 2).
\end{aligned}$$

By induction hypothesis, $\mathcal{P}(t+1)$ is sound. Combining with the facts that $\alpha \neq \beta \in \mathcal{P}(t+1)$ and $y_{\geq e} \in \alpha$, we have $\sum_{x_{\geq e}} \mathrm{ord}_2(y_{\geq e} - x_{\geq e}) = \sum_{x_{\geq e}} \mathrm{ord}_2(y_{\geq e} + x_{\geq e} + t + 2)$, which implies (16).

Case 4.1 $y \in (1^i, 0, ?^{e-1-i}, \alpha)$ and $I = (1^j, 0, ?^{e-1-j}, \beta)$, where $\alpha, \beta \in \mathcal{P}(t)$, and $i \neq j$. The left of (16) is $\min(i, j)|I \cap [0, y-1]|$, and the right of (16) is also $\min(i, j)|I \cap [0, y-1]|$, because $\mathrm{ord}_2((1^i, 0, y_{i+1}, \ldots, y_{e-1}, y_{\geq e}) + (1^j, 0, ?^{e-1-j}, *) + (0^e, t) + (0, 1)) = \min(i, j)$.

Case 4.2 $y \in (1^i, 0, ?^{e-1-i}, \alpha)$ and $I = (1^i, 0, ?^{e-1-i}, \beta)$, where $\alpha \neq \beta \in \mathcal{P}(t)$. The left of (16) is[8]

$$\begin{aligned}
&\sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2((1^i, 0, y_{i+1}, \ldots, y_{e-1}, y_{\geq e}) - (1^i, 0, ?^{e-1-i}, x_{\geq 2})) \\
&= (i+1)|I \cap [0, y-1]| + |\beta \cap [0, k_{\geq e} - 1]| \left(\sum_{j=0}^{e-i-2} j 2^{e-i-j-2} + e - i - 1 \right) \\
&\quad + \sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} - x_{\geq e}),
\end{aligned}$$

where the term $j2^{e-i-j-2}$ corresponds to the sum over $(1^i, 0, y_{i+1}, \ldots, y_{i+j+1}, 1 - y_{i+j+2}, ?^{e-1-i-j}, x_{\geq e})$; the right of (16) is

$$\begin{aligned}
&\sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2((1^i, 0, y_{i+1}, \ldots, y_{e-1}, y_{\geq e}) + (1^i, 0, ?^{e-1-i}, x_{\geq e}) + \\
&(0, 1, 0^{e-2}, t)) \\
&= (i+1)|I \cap [0, y-1]| + |\beta \cap [0, k_{\geq e} - 1]|(\sum_{j=0}^{e-i-2} j 2^{e-i-j-2} + e - i - 1) \\
&\quad + \sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} + x_{\geq e} + t + 1).
\end{aligned}$$

By the soundness of $\mathcal{P}(t)$, and the assumption that $y_{\geq e} \in \alpha, \beta \in \mathcal{P}$ and $\alpha \neq \beta$, we have $\sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} - x_{\geq e}) = \sum_{x_{\geq e} \in \beta \cap [0, y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} + x_{\geq e} + t + 1)$, which proves (16).

[8] In abuse of notation, the term $(1^i, 0, ?^{e-1-i}, x_{\geq 2})$ means the *sum* over all 01 strings by replacing ? by 0 or 1.

Completeness It suffices to prove, for any $y \in I \in \mathcal{P}(2t+1)$ with $\{x \in I : x < y\}$ nonempty,

$$\sum_{x\in I \text{ and } x<y} \mathrm{ord}_2(y-x) < \sum_{x\in I \text{ and } x<y} \mathrm{ord}_2(y+x+2^e t+2). \tag{17}$$

Case 1 $y \in I = (1^e, \alpha)$, where $\alpha \in \mathcal{P}(t+1)$. In this case, the left of (17) is $e|I \cap [0, y-1]| + \sum_{x_{\geq e}\in\alpha}(y_{\geq e} - x_{\geq e})$, and the right of (17) is

$$\sum_{x_{\geq e}\in\alpha\cap[0,y_{\geq e}-1]} \mathrm{ord}_2((1^e, y_{\geq e}) + (1^e, x_{\geq e}) + (0, 1, 0^{e-2}, t))$$

$$= e|I \cap [0, y-1]| + \sum_{x_{\geq e}\in\alpha\cap[0,y_{\geq e}-1]} \mathrm{ord}_2(y_{\geq e} + x_{\geq e} + t + 2).$$

By the completeness of $\mathcal{P}(t+1)$, and the condition $y_{\geq e} \in \alpha \in \mathcal{P}(t+1)$, we have $\sum_{x_{\geq e}}(y_{\geq e} - x_{\geq e}) < \sum_{x_{\geq e}} \mathrm{ord}_2(y_{\geq e} + x_{\geq e} + t + 2)$, which proves (17).

Case 2 $y \in I = (1^i, 0, ?^{e-1-i}, \alpha) \in \mathcal{P}(2^e t+1)$, where $\alpha \in \mathcal{P}(t)$. The left of (17) is

$$\sum_{\substack{x_{i+1},\ldots,x_{e-1}\in\{0,1\},x_{\geq e}\in\alpha \\ :(1^i,0,x_{\geq i+1})<y}} \mathrm{ord}_2((1^i, 0, y_{\geq i+1}) - (1^i, 0, x_{i+1}, \ldots, x_{e-1}, x_{\geq e}))$$

$$= (i+1)|I \cap [0, y-1]| + \sum_{x_{\geq e}\in\alpha} \mathrm{ord}_2((y_{i+1}, \ldots, y_{e-1}, y_{\geq e}) - (?^{e-i-1}, x_{\geq e}))$$

$$+ \sum_{\substack{x_{i+1},\ldots,x_{e-1}\in\{0,1\} \\ :(x_{i+1},\ldots,x_{e-1})<(y_{i+1},\ldots,y_{e-1})}} \mathrm{ord}_2((y_{i+1}, \ldots, y_{e-1}, y_{\geq e}) - (x_{i+1}, \ldots, x_{e-1}, y_{\geq e})).$$

The right of (17) is

$$\sum_{\substack{x_{i+1},\ldots,x_{e-1}\in\{0,1\},x_{\geq e}\in\alpha \\ :(1^i,0,x_{\geq i+1})<y}} \mathrm{ord}_2((1^i, 0, y_{\geq i+1}) + (1^i, 0, x_{\geq i+1}) + (0, 1, 0^{e-2}, t))$$

$$= (i+1)|I \cap [0, y-1]| + \sum_{x_{\geq e}\in\alpha} \mathrm{ord}_2(y_{\geq i+1} + (?^{e-i-1}, x_{\geq e}) + (1, 0^{e-i-2}, t))$$

$$+ \sum_{\substack{x_{i+1},\ldots,x_{e-1}\in\{0,1\} \\ :(x_{i+1},\ldots,x_{e-1})<(y_{i+1},\ldots,y_{e-1})}} \mathrm{ord}_2(y_{\geq i+1} + (x_{i+1}, \ldots, x_{e-1}, y_{\geq e}) + (1, 0^{e-i-2}, t)).$$

Comparing the left with the right, if we could prove

$$\sum_{x_{\geq e}\in\alpha} \mathrm{ord}_2((y_{i+1}, \ldots, y_{e-1}, y_{\geq e}) - (?^{e-i-1}, x_{\geq e}))$$

$$\leq \sum_{x_{\geq e}\in\alpha} \mathrm{ord}_2(y_{\geq i+1} + (?^{e-i-1}, x_{\geq e}) + (1, 0^{e-i-2}, t)) \tag{18}$$

and

$$\sum_{\substack{x_{i+1},\ldots,x_{e-1}\in\{0,1\}\\:(x_{i+1},\ldots,x_{e-1})<(y_{i+1},\ldots,y_{e-1})}} \mathrm{ord}_2((y_{i+1},\ldots,y_{e-1},y_{\geq e})-(x_{i+1},\ldots,x_{e-1},y_{\geq e}))$$

$$\leq \sum_{x_{i+1},\ldots,x_{e-1}} \mathrm{ord}_2(y_{\geq i+1}+(x_{i+1},\ldots,x_{e-1},y_{\geq e})+(1,0^{e-i-2},t)), \tag{19}$$

and "=" in (18), (19) can not hold simultaneously, then (17) will be true.

For (18), the left hand side is

$$|\alpha\cap[0,k_{\geq e}-1]|(\sum_{j=0}^{e-i-2} j2^{e-i-j-2}+e-i-1)+\sum_{x_{\geq e}\in\alpha\cap[0,y_{\geq e}-1]}\mathrm{ord}_2(y_{\geq e}-x_{\geq e}),$$

while the right is

$$|\alpha\cap[0,k_{\geq e}-1]|(\sum_{j=0}^{e-i-2} j2^{e-i-j-2}+e-i-1)+\sum_{x_{\geq e}\in\alpha\cap[0,y_{\geq e}-1]}\mathrm{ord}_2(y_{\geq e}+t+1).$$

By the induction hypothesis that $\mathcal{P}(t)$ is complete, we have

$$\sum_{x_{\geq e}\in\alpha\cap[0,y_{\geq e}-1]}\mathrm{ord}_2(y_{\geq e}-x_{\geq e})\leq\sum_{x_{\geq e}\in\alpha\cap[0,y_{\geq e}-1]}\mathrm{ord}_2(y_{\geq e}+t+1),$$

where the $\leq$ is strictly less if $\alpha\cap[0,k_{\geq e}-1]$ is nonempty.

For (19), the left is $\sum_{x=0}^{y'-1}\mathrm{ord}_2(y'-x)=\mathrm{ord}_2(y'!)$, where $y'=(y_{i+1},\ldots,y_{e-1})$, and the right is at least $\sum_{x=0}^{y'-1}\mathrm{ord}_2(y'+x+1)=\mathrm{ord}_2((2y')!/y'!)$. From (11), we know $\mathrm{ord}_2(y')\leq\mathrm{ord}_2((2y')!/y'!)$ unless $y'=0$. Suppose for contradiction that the "=" holds in both (18) and (19) are true. Then $y'=(y_{i+1},\ldots,y_{e-1})=0$ and $\alpha\cap[0,y_{\geq e}-1]$ is empty, which implies $I\cap[0,y-1]$ is empty, which contradicts our assumption!

5 Proof for the case char($\mathbb{F}$) $\geq$ 3

For the case $p\geq 3$, the idea of proving Lemma 4 is similar to that of $p=2$. And the construction of $\mathcal{P}(\mathbb{F}_p,t)$ is in some sense simpler, where fewer cases are involved.

Within the section, p is always a prime greater than 2, and let $q=(p+1)/2$. For convenience, we may write $\mathcal{P}(t)$ instead of $\mathcal{P}(\mathbb{F}_p,t)$, and we adopt the same p-adic expansion notation used in the last section.

Definition 4 Let $p\geq 3$ be a prime, and $q=(p+1)/2$. Define

$$\mathcal{P}(0)=\{(\{x_0,p-1-x_0\},\{x_1,p-1-x_1\},\ldots)_p:0\leq x_i\leq q-1\}$$

and

$$\mathcal{P}(1)=\{((p-1)^i,\{j,p-2-j\},\alpha)_p:\alpha\in\mathcal{P}(0),i\geq 0,j=0,1,\ldots,q-2\},$$

where $\{j,p-2-j\}$ denotes a bit which is either j or $p-2-j$. For any integer $t\geq 0$ and $0\leq r\leq p-1$ with $pt+r\geq 2$, define

$$\mathcal{P}(pt+r)$$
$$=\{(\{i,j\},\alpha)_p:0\leq i,j\leq p-1,b\in\{1,2\},i+j+r+1=bp,\alpha\in\mathcal{P}(t+b-1)\}.$$

To help understand the definition, let us redefine the partition in standard set notations instead of "patterns". Partition $\mathcal{P}(0) = \{I_0, I_1, \ldots\}$, where

$$\begin{aligned} I_j &= \{x = (x_0, x_1, \ldots)_p : \sum_{i:x_i \le q-1} x_i q^i + \sum_{i:x_i \ge q} (p-1-x_i)q^i = j\}. \\ \mathcal{P}(1) &= \{(p^{i+1}I + jp^i + p^i - 1) \cup (p^{i+1}I + (p-2-j)p^i + p^i - 1) : \\ &\quad I \in \mathcal{P}(0), i \ge 0, j = 0, 1, \ldots, q-2\}. \\ \mathcal{P}(pt+r) &= \{(i + pI) \cup (j + pI) : 0 \le i, j \le p-1, b \in \{1,2\}, i + j + r + 1 = bp, \\ &\quad I \in \mathcal{P}(t + b - 1)\}. \end{aligned}$$

5.1 $\mathcal{P}(\mathbb{F}_p, 0)$

By the definition of $\mathcal{P}(0)$, every set in $\mathcal{P}(0)$ is uniquely identified by some pattern $(\{x_0, p-1-x_0\}, \{x_1, p-1-x_1\}, \ldots)_p$, where $x_0, x_1, \ldots \in \{0, 1, \ldots, q-1\}$.

Soundness It suffices to prove, for any $y \notin I = (\{z_0, p-1-z_0\}, \{z_1, p-1-z_1\}, \ldots)_p$,

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y-x) = \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y+x+1). \tag{20}$$

Let i be the minimum index such that $y_i \notin \{z_i, p-1-z_i\}$. (By assumption that $y \notin I$, such i exists.) It is not difficult to see both the left and the right of (20) is

$$|(\{z_i, p-1-z_i\}, \{z_{i+1}, p-1-z_{i+1}\}, \ldots)_p \cap [0, y_{\ge i} - 1]| \left(\sum_{j=1}^{i-1} j 2^{i-j-1} + i \right).$$

Completeness It suffices to prove, for any $y \in I$ with $I \cap [0, y-1]$ nonempty,

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y-x) < \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y+x+1). \tag{21}$$

Let $I = (\{z_0, p-1-z_0\}, \{z_1, p-1-z_1\}, \ldots)_p$. Let i be an integer such that $z_i = (p-1)/2$. The ith bit on the left of (21) is zero if $x_j = y_j$ for all $j \le i$, and $x_{\ge j} < y_{\ge j}$; and the ith bit on the right is zero if $x_j = p-1-y_j$ for all $j \le i$, and $x < y$, which *includes* the case $x_{\ge j} < y_{\ge j}$. By a double counting argument, without loss of generality, assume such i does not exists, that is, for all i, $z_i \ne (p-1)/2$.

Let $\phi : \mathbb{Z}_{\ge 0} \to \mathbb{Z}_{\ge 0}$ be the map

$$\phi(x) = (x'_0, x'_1, \ldots)_2,$$

where $x = (x_0, x_1, \ldots)_p$ is the p-adic expansion of x, and $x'_i = 1$ if and only if $x_i = \max(x_i, p-1-x_i)$, otherwise 0. Then, under our assumption that $x_i \ne (p-1)/2$ for all i, (21) becomes

$$\sum_{x \in [0, \phi(y)-1]} \mathrm{ord}_2(\phi(y) - x) < \sum_{x \in [0, \phi(y)-1]} \mathrm{ord}_2(\phi(y) + x + 1),$$

which is equivalent to $\mathrm{ord}_2(\phi(y)!) < \mathrm{ord}_2((2\phi(y))!/\phi(y)!)$, which is exactly (11).

5.2 $\mathcal{P}(\mathbb{F}_p, 1)$

Soundness We shall prove for any $y \notin I = ((p-1)^i, \{j, p-2-j\}, \alpha)_p$, $j < p-2-j$, where $y \in ((p-1)^{i'}, \{j', p-2-j'\}, \beta)_p$, and $\alpha, \beta \in \mathcal{P}(0)$,

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y-x) = \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y+x+2). \tag{22}$$

Case 1 $i \neq i'$. Both the left and right of (22) are $\min(i, i')|I \cap [0, y-1]|$.

Case 2 $i = i'$ and $j \neq j'$. Both the left and right of (22) are $i|I \cap [0, y-1]|$.

Case 3 $i = i'$, $j = j'$ and $\alpha \neq \beta$. The left of (22) is

$$(i+1)|\alpha \cap [0, y_{\geq i+1}]| + \sum_{x_{\geq i+1} \in \alpha \cap [0, y_{\geq i+1}]} \mathrm{ord}_p(y_{\geq i+1} - x_{\geq i+1}),$$

and the right of (22) is

$$(i+1)|\alpha \cap [0, y_{\geq i+1}]| + \sum_{x_{\geq i+1} \in \alpha \cap [0, y_{\geq i+1}]} \mathrm{ord}_p(y_{\geq i+1} + x_{\geq i+1} + 1).$$

Since $\mathcal{P}(0)$ is sound, and $y_{\geq i+1} \notin \alpha \in \mathcal{P}(0)$, we have $\sum_{x_{\geq i+1}} \mathrm{ord}_p(y_{\geq i+1} - x_{\geq i+1}) = \sum_{x_{\geq i+1}} \mathrm{ord}_p(y_{\geq i+1} + x_{\geq i+1} + 1)$, which implies (22).

Completeness We need to prove for any $y \in I = ((p-1)^i, \{j, p-2-j\}, \alpha)_p \in \mathcal{P}(1)$ with $I \cap [0, y-1]$ nonempty,

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y-x) < \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y+x+2). \tag{23}$$

The left side of (23) is

$$\sum_{x_i \in \{j, p-2-j\}, x_{\geq i+1} \in \alpha : x < y} \mathrm{ord}_p(((p-1)^i, y_i, y_{\geq i+1})_p - ((p-1)^i, x_i, x_{\geq i+1})_p)$$
$$= (2i+1)|\alpha \cap [0, y_{\geq i+1} - 1]| + i\delta_{y_i, p-2-j} + \sum_{\substack{x_{\geq i+1} \in \alpha \\ x_{\geq i+1} < y_{\geq i+1}}} \mathrm{ord}_p(y_{\geq i+1} - x_{\geq i+1}),$$

and the right of (23) is

$$\sum_{x_i \in \{j, p-2-j\}, x_{\geq i+1} \in \alpha : x < y} \mathrm{ord}_p(((p-1)^i, y_i, y_{\geq i+1})_p + ((p-1)^i, x_i, x_{\geq i+1})_p + 2)$$
$$\geq (2i+1)|\alpha \cap [0, y_{\geq i+1} - 1]| + (i+1)\delta_{y_i, p-2-j} + \sum_{\substack{x_{\geq i+1} \in \alpha \\ x_{\geq i+1} < y_{\geq i+1}}} \mathrm{ord}_p(y_{\geq i+1} + x_{\geq i+1} + 1).$$

Since $\mathcal{P}(0)$ is complete, we have

$$\sum_{x_{\geq i+1} \in \alpha} \mathrm{ord}_p(y_{\geq i+1} - x_{\geq i+1}) < \sum_{x_{\geq i+1} \in \alpha} \mathrm{ord}_p(y_{\geq i+1} + x_{\geq i+1} + 1)$$

if $\alpha \cap [0, y_{\geq i+1} - 1]$ is not empty, in which (23) is true. Otherwise, by assumption $I \cap [0, y-1]$ is nonempty, we have $y_i = p-2-j$, which also implies (23).

5.3 $\mathcal{P}(\mathbb{F}_p, pt + r)$

By definition, $\mathcal{P}(pt + r) = \{(\{i, j\}, \alpha)_p : 0 \le i, j \le p - 1, b \in \{1, 2\}, i + j + r + 1 = bp, \alpha \in \mathcal{P}(t + b - 1)\}$.

Soundness We will prove for any $y \notin I = (\{i', j'\}, \beta)_p \in \mathcal{P}(pt + r)$, where $y \in (\{i, j\}, \alpha)_p$,

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y - x) = \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y + x + pt + r + 1). \tag{24}$$

Without loss of generality, assume $i = i'$ and $j = j'$, otherwise both sides of (24) are 0. By definition, $i + j + r + 1 = bp$, where $b \in \{1, 2\}$, and $\alpha \ne \beta \in \mathcal{P}(t + b - 1)$. The left hand side of (24) is

$$|I \cap [0, y - 1]| + \sum_{x_{\ge 1} \in \beta \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p(y_{\ge 1} - x_{\ge 1}),$$

and the right of (24) is

$$\sum_{x_{\ge 1} \in \beta \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p((y_0, y_{\ge 1})_p + (\{i, j\}, x_{\ge 1})_p + (r + 1, t)_p)$$
$$= |I \cap [0, y - 1]| + \sum_{x_{\ge 1} \in \beta \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p(y_{\ge 1} + x_{\ge 1} + t + b).$$

By induction hypothesis, $\mathcal{P}(t + b - 1)$ is sound, we have $\sum_{x_{\ge 1}} \mathrm{ord}_p(y_{\ge 1} - x_{\ge 1}) = \sum_{x_{\ge 1}} \mathrm{ord}_p(y_{\ge 1} + x_{\ge 1} + t + b)$, which proves (24).

Completeness We prove, for any $y \in I = (\{i, j\}, \alpha) \in \mathcal{P}(pt + r)$ with $I \cap [0, y - 1]$ nonempty, and $i < j$,

$$\sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y - x) < \sum_{x \in I \cap [0, y-1]} \mathrm{ord}_p(y + x + pt + r + 1), \tag{25}$$

where $i + j + r + 1 = bp$, $b \in \{1, 2\}$, and $\alpha \in \mathcal{P}(t + b - 1)$. The left of (25) is

$$|\alpha \cap [0, y_{\ge 1} - 1]| + \sum_{x_{\ge 1} \in \alpha \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p(y_{\ge 1} - x_{\ge 1}),$$

and the right of (25) is

$$\sum_{x_{\ge 1} \in \alpha \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p((y_0, y_{\ge 1})_p + (\{i, j\}, x_{\ge 1})_p + (r + 1, t)_p)$$
$$\ge |\alpha \cap [0, y_{\ge 1} - 1]| + \delta_{y_0, j} + \sum_{x_{\ge 1} \in \alpha \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p(y_{\ge 1} + x_{\ge 1} + t + b).$$

By the induction hypothesis that $\mathcal{P}(t + b - 1)$ is complete, then

$$\sum_{x_{\ge 1} \in \alpha \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p(y_{\ge 1} - x_{\ge 1}) < \sum_{x_{\ge 1} \in \alpha \cap [0, y_{\ge 1} - 1]} \mathrm{ord}_p(y_{\ge 1} + x_{\ge 1} + t + b)$$

if $\alpha \cap [0, y_{\ge 1} - 1]$ is nonempty, in which case (25) is true; otherwise, $y_0 = j > i$, which also implies (25).

The author would like to thank Alexander Razborov for helpful discussions which make the author consider general t in Theorem 1, and thank anonymous reviewers for their comments and suggestions which improve the presentation.

References

1. Alekhnovich, M., Razborov, A.: Lower bounds for polynomial calculus non binomial case. In: 42nd IEEE Symposium on Foundations of Computer Science, pp. 190–199 (2001)
2. An, B., Preneel, B.: On the algebraic immunity of symmetric boolean functions. In: Progress in Cryptology—Indocrypt 2004, LNCS 3797, pp. 35–48 (2005)
3. Beck, C., Li, Y.: Represent MOD function by low degree polynomial with unbounded one-sided error. arXiv:1304.0713 (2013)
4. Carlet, C., Dalai, D.K., Gupta, K.C., Maitra, S.: Algebraic immunity for cryptographically significant boolean functions: analysis and construction. IEEE Trans. Inf. Theory **52**(7), 3105–3121 (2006)
5. Carlet, C., Feng, K.: An infinite class of balanced functions with optimum algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Proceedings of ASIACRYPT 2008, LNCS 5350, pp. 425–440 (2008)
6. Courtois, N.T., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology—EUROCRYPT 2003, LNCS 2656, pp. 346–359 (2003)
7. Chaudhuri, S., Radhakrishnan, J.: Deterministic restrictions in circuit complexity. STOC 96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 30–36. ACM Press (1996)
8. Green, F.: A complex-number Fourier technique for lower bounds on the Mod-m degree. Comput. Complex. **9**(1), 16–38 (2000)
9. Kopparty, S., Srinivasan, S.: Certifying polynomials for AC0[$\oplus$] circuits, with applications. In: 32nd Intl Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2012), pp. 36–47
10. Liu, F., Feng, K.: Efficient computation of algebraic immunity of symmetric boolean functions. LNCS **4484**, 318–329 (2007)
11. Na, L., Qi, W.: Symmetric boolean functions depending on an odd number of variables with maximum algebraic immunity. IEEE Trans. Inf. Theory **52**(5), 2271–2273 (2006)
12. Pasalic, E.: A design of boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation. Cryptogr. Commun. **4**(1), 25–45 (March 2012)
13. Peng, J., Quanshui, W., Kan, H.: On symmetric boolean functions with high algebraic immunity on even number of variables. IEEE Trans. Inf. Theory **57**(10), 7205–7220 (2011)
14. Longjiang, Q., Li, C.: On the 2^m-variable symmetric boolean functions with maximum algebraic immunity. Sci. China Ser. F: Inf. Sci. **51**(2), 120–127 (2008)
15. Tang, D., Carlet, C., Tang, X.: Highly nonlinear boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. IEEE Trans. Inf. Theory **59**(1), 653–664 (2013)
16. Wang, H.ui., Peng, J.ie., Li, Y.uan., Kan, H.aibin.: On 2k-variable symmetric boolean functions with maximum algebraic immunity k. IEEE Trans. Inf. Theory **58**(8), 5612–5624 (2012)