Towards the Least Inequalities for Describing a Subset in $\mathbb{F}_2^n$

Yao Sun

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.
School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China.
sunyao@iie.ac.cn

Abstract. Mixed Integer Linear Programming (MILP) solvers have become one of the most powerful tools for searching cryptographic characteristics, including differentials, impossible differentials, and division trails. Generally, one MILP problem can be formulated by several different MILP models, and the models with fewer constraints and variables are usually easier to solve. How to model a problem with the least number of constraints is also an interesting mathematical problem. In this paper, we discuss this problem in a general form. Specifically, given a set $C \subset \mathbb{F}_2^n$, let L be a set of inequalities, and we say L describes C if the inequalities in L only involve n variables and the solution set to L is exactly C. Our goal is to find such a set L with the least number of inequalities. We present a brand new approach, named as SuperBall approach, for resolving this problem completely. Our approach is able to generate all available inequalities. Once these inequalities are obtained, Sasaki and Todo's method is used to find out the smallest subset of inequalities that describes C. If Sasaki and Todo's method succeeds, the found subset will be proved as the smallest. As a result, we found the smallest subsets of inequalities that describe the Sboxes of KECCAK and APN-6. The previous best results were 34 and 167, presented in FSE 2020, and we decreased these numbers to 26 and 145. Moreover, we can prove these numbers are the smallest in case no dummy variables are involved.

Keywords: MILP · inequalities · Sbox.

1 Introduction

In this paper, we consider the following mathematical problem.

Problem: Let C be a subset of $\mathbb{F}_2^n$ where $\mathbb{F}_2$ is the field with two elements $\{0, 1\}$. We say a set L of inequalities **describes** the set C, if the inequality in L involves n variables and the solutions to L is exactly C. The problem is how to find a set L_{min} such that L_{min} describes C and for any L that describs C we always have $|L_{min}| \leq |L|$, where $|L|$ means the cardinality of L.

This problem can be illustrated by Figure 1. $\mathbb{F}_2^n$ is the set of all n-dim vectors. Every n-dim vector can be seen as a **point**, and all the points in $\mathbb{F}_2^n$ are

represented as white and black points in Figure 1. Let C be the set of the 5 black points. A line stands for an inequality, and the solutions of this inequality lie in only one side of the line. In this figure, L contains 4 inequalities, and the solutions are exactly the set C. The problem is to find the least number of inequalities to describe C.

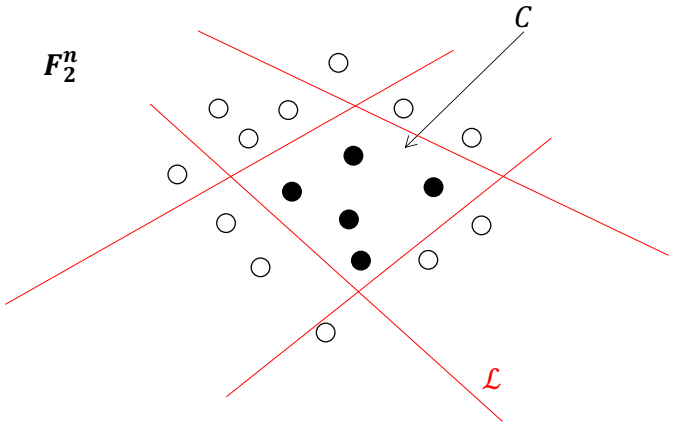

Fig. 1. Illustration of the problem.

In many cryptographic problems, we need to construct inequalities to describe a set of points, e.g. formulating Difference Distribution Table (DDT) or Division property by Mixed Integer Linear Programming (MILP) models. Generally, fewer constraints make the MILP models easier to solve. Thus, the above problem makes senses in many cryptographic analysis.

Traditional methods trade the above problem as two sub-problems.

Problem 1 How to generate a (possibly large) set of inequalities in n variables such that the solution set of every inequality contains C.

Problem 2 How to choose a (typically much smaller) subset of the obtained set of inequalities such that this subset exactly describes the set C.

Many works have been done for resolving the above two sub-problems. For Problem 1, two different approaches were proposed by Sun et al. [SHW+14a] [SHW+14b]. These methods were first improved by Abdelkhalek et al. [AST+17] and then further developed by Boura and Coggia in [BC20]. In [BC20], *balls* and *distorted balls* were used to generate inequalities, and by combining different inequalities via algebraic operations, they could also construct many more inequalities than previous works. For Problem 2, Sun et al. proposed a greedy method in [SHW+14a] [SHW+14b]. This method was improved by Sasaki and Todo in [ST17] by using an MILP-based method. In this paper, we only consider Problem 1, and use Sasaki and Todo's approach to solve the second sub-problem.

Contribution We propose a brand new approach, called SuperBall approach, to generate all available inequalities for a given set of points. In [BC20], a ball is a set of points in $\mathbb{F}_2^n$ and contains a point $c \in \mathbb{F}_2^n$ as well as all the points $x \in \mathbb{F}_2^n$ such that the Hamming distance between c and x is smaller than a fixed radius d. Distorted balls were obtained by merging balls that have some special structures. The authors proposed several methods of constructing inequalities for balls and distorted balls. The limitation of their methods is the points in balls or distorted balls must have some special structures, and this means if a set of points does not have such special structures, their methods cannot construct inequalities. But our SuperBall method does not have such requirements. We name our method as SuperBall, because the set of solutions to our generated inequalities could form some peculiar-looking "balls". That is, the set of solutions to our inequalities could have very flexible form. This difference enables us to obtain all available inequalities via the SuperBall approach. Besides, our SuperBall approach constructs inequalities in a quite different way from those in [BC20], and this will be introduced in Section 3.

Once all the available inequalities are obtained, we can apply Sasaki and Todo's method to obtain the minimal set of inequalities by Gurobi [GO21]. As a result, we significantly improved some results in [BC20], as shown in Table 1. More importantly, we can also prove the numbers of inequalities are the smallest, if no dummy variables are introduced.

			# Inequalities				
n	Sbox	Citation	Convex Hull	Alg.2	Alg. 1	Alg. 3*	our results
10	Keccak	[BDPA11]	46	46	34	36	**26**
12	APN-6	[BDMW10][Dil09]	195	288	167	179	**145**

Table 1. Main results of our SuperBall approach. "Alg. 1", "Alg. 2", and "Alg. 3*" are the algorithms from [BC20], where "Alg. 3*" is short for "Alg. 2 and 3 and Prop. 3".

2 Preliminary

Let $\mathbb{F}_2^n$ be the set of all n-dim vectors, and the entries of the vectors belong to the field $\mathbb{F}_2 = \{0, 1\}$. For convenience, we also call the n-dim vectors in $\mathbb{F}_2^n$ as **points**. Let f be a linear polynomial in $\mathbb{Z}[x_0, x_1, \ldots, x_{n-1}]$, then an **inequality** in n variables can be represented as $f \geq 0$, where $f = a_0x_0 + a_1x_1 + \cdots + a_{n-1}x_{n-1} + a_n$ and $a_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, n$. For any given point $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, $f(\mathbf{c}) = a_0c_0 + \cdots + a_{n-1}c_{n-1} + a_n \in \mathbb{Z}$. If $f(\mathbf{c}) \geq 0$, then $\mathbf{c}$ is a solution to the inequality $f \geq 0$, or for convenience, we say the inequality $f \geq 0$ **contains** $\mathbf{c}$; otherwise, we say $f \geq 0$ **excludes** $\mathbf{c}$ if $f(\mathbf{c}) < 0$.

For example, let $f = -3x_0 - 2x_1 + x_2 + 4x_3 + 3 \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ and $(0,0,1,1), (1,1,0,0) \in \mathbb{F}_2^4$ are two points, then we have $f \geq 0$ contains $(0,0,1,1)$ and excludes $(1,1,0,0)$, because $f(0,0,1,1) = 7$ and $f(1,1,0,0) = -2$.

To study the inequalities in n variables in more details, we can transform the above f to another form below:

$$f = 3(1 - x_0) + 2(1 - x_1) + x_2 + 4x_3 - 2.$$

Note that, since $x_i \in \mathbb{F}_2$, we also have $1 - x_i \in \mathbb{F}_2$. This form is called "logical condition modeling" of f and was proposed by Sun et al. [SHW+14a] [SHW+14b]. Let $\bar{x}_0 = (1 - x_0)$, $\bar{x}_1 = (1 - x_1)$, $\bar{x}_2 = x_2$, and $\bar{x}_3 = x_3$. We have

$$f = 3\bar{x}_0 + 2\bar{x}_1 + \bar{x}_2 + 4\bar{x}_3 - 2. \tag{1}$$

Since the coefficients of $\bar{x}_i$'s are all non-negative, then f gets its smallest value at the point $(1,1,0,0)$. Moreover, the polynomial $a_0\bar{x}_0 + a_1\bar{x}_1 + a_2\bar{x}_2 + a_3\bar{x}_3 - d$ always gets its smallest value at the point $(1,1,0,0)$ where $a_i \geq 0$ for $i = 0,1,2,3$. We call the point $(1,1,0,0)$ as the **center** of the above f. As any inequality can be transformed to the form like Eq. (1), any inequality has a center. Be careful that, an inequality may have multiple centers if the coefficient of some $\bar{x}_i$ is 0.

Conversely, given a point $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$, all the inequalities, whose center is $\mathbf{c}$, can be formulated as the following form

$$a_0\bar{x}_0 + a_1\bar{x}_1 + \cdots + a_{n-1}\bar{x}_{n-1} - d \geq 0, \tag{2}$$

where $a_i \geq 0, i = 0, 1, \ldots, n-1$, and

$$\bar{x}_i = \begin{cases} x_i & c_i = 0, \\ 1 - x_i & c_i = 1. \end{cases}$$

Inequalities in the form Eq. (2) are easier to be studied, because all the coefficients of $\bar{x}_i$ are not negative. Particularly, we can also require $d \geq 0$, because the inequality (2) contains all points in $\mathbb{F}_2^n$ and makes no senses.

In [SHW+14a] [SHW+14b], the authors consider the special case of Eq. (2) by setting $a_0 = a_1 = \cdots = a_{n-1} = d = 1$. In this case, this inequality contains all the points in $\mathbb{F}_2^n$ except the point $\mathbf{c}$. Boura and Coggia considered the case $a_0 = a_1 = \cdots = a_{n-1} = 1$ and $d > 1$ in [BC20], and in this case, this inequality could exclude the point $\mathbf{c}$ as well as all the points $\mathbf{b}$ where the Hamming distance between $\mathbf{c}$ and $\mathbf{b}$ is not bigger than d. In our SuperBall approach, the values of a_i and d will have more flexible choices, such that we can construct more kinds of inequalities.

3 The SuperBall approach

Definition 1. *Let $\mathbb{F}_2^n$ be the set of all points, and $C \subset \mathbb{F}_2^n$ be the set of points we need to describe. Denote $E = \mathbb{F}_2^n \setminus C$.*

We say an inequality $f \geq 0$ is **available** *for C if $f \geq 0$* contains *all points in C and* excludes *some points in E.*

For two available inequalities $f \geq 0$ and $g \geq 0$ for C, we say $f \geq 0$ **covers** *$g \geq 0$, if the points excluded by $g \geq 0$ is a subset of the points that are excluded by $f \geq 0$.*

Let F be a set of inequalities, we say F is **complete** *for C if for any available inequality $g \geq 0$, there exists an inequality $f \geq 0 \in F$ such that $f \geq 0$ covers $g \geq 0$.*

The above notations will be used throughout this section.

It is not difficult to see that, if we have got a complete set F for C and we can calculate the optimal solution by using Sasaki and Todo's approach, then this optimal solution leads to a provable smallest set of inequalities that describes C. Please remark that, if the size of F is too large, say $\geq 1,000,000$, Sasaki and Todo's approach may not calculate the optimal solution within endurable time due to the high complexity.

The SuperBall approach is able to compute a complete inequality set. For each point $\mathbf{c} \in \mathbb{F}_2^n \setminus C$, we generate all available inequalities whose center is $\mathbf{c}$ by the following three steps.

1. We compute the **region** of $\mathbf{c}$ (see Definition 2), and denote it as $\text{Region}(\mathbf{c}) \subset \mathbb{F}_2^n$. For any point that is not in $\text{Region}(\mathbf{c})$, it cannot be excluded by any available inequality whose center is $\mathbf{c}$. More details about $\text{Region}(\mathbf{c})$ can be found in SubSection 3.1. Generally, the size of $\text{Region}(\mathbf{c})$ is much smaller than the size of $E = \mathbb{F}_2^n \setminus C$.
2. We calculate an available inequality whose center is $\mathbf{c}$, such that this inequality can exclude as many points in $\text{Region}(\mathbf{c})$ as possible. This can be done by regarding the coefficients in Eq. (2) as unknowns and then solving an MILP model. Details can be found in SubSection 3.2.
3. If we get an inequality by Step 2, we remove this inequality as well as the inequalities it covers in the further computation, and then jump to Step 2; otherwise, we have got all the available inequalities whose center is $\mathbf{c}$ and the computation is done. Related details come in SubSection 3.3.

In this way, a complete inequality set can be obtained by repeating the above three steps for every $\mathbf{c} \in \mathbb{F}_2^n \setminus C$.

3.1 The region of a point c

Definition 2. *Given a point $\mathbf{c} \in \mathbb{F}_2^n \setminus C$, we say a set R is the* **region** *of $\mathbf{c}$, if for any point $\mathbf{b} \in \mathbb{F}_2^n \setminus (C \cup R)$, $\mathbf{b}$ cannot be excluded by any inequality whose center is $\mathbf{c}$. We denote R as* $\text{Region}(\mathbf{c})$.

The concept of the region is new, and to make it easier understood, we use the following example for an illustration.

Example 1. Let $C = \{1101, 1010, 1001, 0101, 0010\} \subset \mathbb{F}_2^4$, where 1101 is short for the vector $(1, 1, 0, 1) \in \mathbb{F}_2^4$, and $\mathbf{c} = 1100 \in \mathbb{F}_2^4$. We next compute the region of $\mathbf{c}$.

By definition, we have $E = \mathbb{F}_2^4 \setminus C = \{1100, 0100, 1000, 1110, 0000, 0110, 1111, 1011, 0111, 0011\}$. Note that all inequalities whose center is 1100 have the following form

$$a_0(x_0 - 1) + a_1(x_1 - 1) + a_2x_2 + a_3x_3 - d \geq 0,$$

or equivalently,

$$a_0\bar{x}_0 + a_1\bar{x}_1 + a_2\bar{x}_2 + a_3\bar{x}_3 - d \geq 0, \tag{3}$$

where $\bar{x}_0 = 1 - x_0$, $\bar{x}_1 = 1 - x_1$, $\bar{x}_2 = x_2$, and $\bar{x}_3 = x_3$ and $a_i \geq 0$ for $i = 0, 1, 2, 3$.

In fact, $\bar{x}_0\bar{x}_1\bar{x}_2\bar{x}_3$ is just $x_0x_1x_2x_3 \oplus 1100$. To use Eq (3), we would better use the relative coordinates of each points with respect to $\mathbf{c} = 1100$. That is, we consider $\bar{C} = C \oplus \mathbf{c} = \{0001, 0110, 0101, 1001, 1110\}$, and similarly, $\bar{E} = E \oplus \mathbf{c} = \{0000, 1000, 0100, 0010, 1100, 1010, 0011, 0111, 1011, 1111\}$. In this case, $\bar{\mathbf{c}} = \mathbf{c} \oplus \mathbf{c} = 0000$. In the rest of this subsection, we always use relative coordinates of points for simplification. An inequality writing in relative coordinates can be transformed back to the absolute coordinates easily.

Let $\bar{f} = a_0\bar{x}_0 + a_1\bar{x}_1 + a_2\bar{x}_2 + a_3\bar{x}_3 - d \geq 0$ be an inequality whose center is $\mathbf{c}$ where $a_i \geq 0$ for $i = 0, 1, 2, 3$. Let us see which conditions $\bar{f}$ should meet, if $\bar{f} \geq 0$ is an available inequality for $\bar{C}$. By definition, $\bar{f} \geq 0$ must contain all the points in $\bar{C}$. That is, we must have

$$\bar{f}(0001) = a_3 - d \geq 0,$$

$$\bar{f}(1001) = a_0 + a_3 - d \geq 0,$$

$$\bar{f}(0110) = a_1 + a_2 - d \geq 0,$$

$$\bar{f}(0101) = a_1 + a_3 - d \geq 0,$$

$$\bar{f}(1110) = a_0 + a_1 + a_2 - d \geq 0.$$

With these hard conditions, can every point in $\bar{E}$ be excluded by $\bar{f}$? The answer is NO. Take the point $0011 \in \bar{E}$ for an example, we have

$$\bar{f}(0011) = a_2 + a_3 - d.$$

Because we have $\bar{f}(0001) = a_3 - d \geq 0$ and $a_2 \geq 0$, this means $\bar{f}(0011) \geq 0$ and hence, the point 0011 cannot be excluded by $\bar{f}$ whatever the coefficients of $\bar{f}$ are. So do the points 1011, 1101, 0111, and 1111. Removing the points in similar cases, we can obtain the region of 0000 which is $\{0000, 1000, 0100, 0010, 1100, 1010\}$. Please note that the size of Region(0000) is 6 which is smaller than the size of $\bar{E}$.

To compute the region of a center point, we introduce the following definition.

Definition 3. *For two points* $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}), \mathbf{b} = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_2^n$, *we say* $\mathbf{a} \preceq \mathbf{b}$ *if* $a_i \leq b_i$ *for* $i = 0, 1, \ldots, n-1$. *We denote the set* $\{\mathbf{a} \preceq \mathbf{b} \mid \mathbf{a} \in \mathbb{F}_2^n\}$ *as* $\mathrm{Prec}(\mathbf{b})$.

Next, we present the key theorem of the SuperBall approach.

Theorem 1. *Let $\bar{f} = a_0\bar{x}_0 + a_1\bar{x}_1 + \cdots + a_{n-1}\bar{x}_{n-1} - d$ be a linear polynomial where $a_i \geq 0$ for $i = 0, 1, \ldots, n-1$, and $\bar{f} \geq 0$ is an inequality having a center $\mathbf{0} \in \mathbb{F}_2^n$. For two points $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{F}_2^n$, if $\mathbf{b}_1 \preceq \mathbf{b}_2$, then we must have $\bar{f}(\mathbf{b}_1) \leq \bar{f}(\mathbf{b}_2)$. Particularly, if $\bar{f} \geq 0$ contains the point $\mathbf{b}_1$, then $\bar{f} \geq 0$ also contains the point $\mathbf{b}_2$; if $\bar{f} \geq 0$ excludes the point $\mathbf{b}_2$, then $\bar{f} \geq 0$ also excludes the point $\mathbf{b}_1$.*

The proof of the above theorem is straightforward. Besides, we have the following corollary.

Corollary 1. *If $\mathbf{b} \in \mathrm{Region}(\mathbf{0})$, then for any $\mathbf{b}_0 \preceq \mathbf{b}$, we have $\mathbf{b}_0 \in \mathrm{Region}(\mathbf{0})$.*

Corollary 2. *If $\mathbf{b} \in \bar{C}$, then for any $\mathbf{b} \preceq \mathbf{b}_1$, we have $\mathbf{b}_1 \notin \mathrm{Region}(\mathbf{0})$.*

Corollary 3. $\mathrm{Region}(\mathbf{0}) = \mathrm{Prec}(\mathbf{b_1}) \cup \mathrm{Prec}(\mathbf{b_2}) \cup \cdots \cup \mathrm{Prec}(\mathbf{b_l})$, *where $\mathbf{b}_i$ is some point in $\mathbb{F}_2^n$ for $i = 1, 2, \ldots, l$.*

Using Corollary 1 and 2, we can compute the region of $\mathbf{0}$ efficiently. The points $\mathbf{b}_i$'s in Corollary 3 give a shape of the region, so we usually call these $\mathbf{b}_i$'s **border** points. In fact, the solution set to our constructed inequalities has a similar shape as described in Corollary 3. There is a center inside this solution set as well as a few border points. The points between the borders and the center can all be excluded, so the shape of this solution set likes a peculiar-looking "ball". This is why we call our approach as SuperBall approach.

3.2 Compute the maximal available inequality inside a region

In this subsection, we present an algorithm for computing the maximal available inequality inside a region. Again, relative coordinates are used, so the region in consider is $\mathrm{Region}(\mathbf{0})$.

Let $\bar{f} = a_0\bar{x}_0 + a_1\bar{x}_1 + \cdots + a_{n-1}\bar{x}_{n-1} - d$ be a linear polynomial where $a_i \geq 0$ for $i = 0, 1, \ldots, n-1$, and $\bar{f} \geq 0$ is an inequality having a center $\mathbf{0} \in \mathbb{F}_2^n$. To determine the polynomial $\bar{f}$, it suffices to determine the values of a_i and d for $i = 0, 1, \ldots, n-1$. Beside, we also hope the inequality $\bar{f} \geq 0$ could exclude as many points in $\mathrm{Region}(\mathbf{0})$ as possible. For this goal, we can build an MILP model and solve it by Gurobi.

Specifically, this MILP model contains two types of constraints. Firstly, $\bar{f} \geq 0$ should be an available inequality for C, so for any point $\mathbf{b} \in C$, we add the following constraint to the model

$$\bar{f}(\mathbf{b}) \geq 0.$$

Secondly, for each point $\mathbf{b} \in \mathrm{Region}(\mathbf{0})$, we assign a binary variable $z_{\mathbf{b}}$ associated to $\mathbf{b}$, and add the following constraint to the model

$$\bar{f}(\mathbf{b}) - A(1 - z_{\mathbf{b}}) < 0,$$

where A is a large integer such that $A > a_0 + a_1 + \cdots + a_{n-1}$. With this setting, if $z_{\mathbf{b}} = 1$, then the point $\mathbf{b}$ is excluded by $\bar{f} \geq 0$; otherwise, the above constraint makes no sense. The object function of the model is

$$\text{Maximize} \sum_{\mathbf{b} \in \text{Region}(\mathbf{0})} z_{\mathbf{b}}.$$

If the size of Region($\mathbf{0}$) is only a few hundreds, the above model can be solved by Gurobi in seconds.

3.3 Remove the inequality as well as the inequalities it covers

In order to avoid duplicated computations, if we have got an inequality by the algorithm in SubSection 3.2, we should remove this inequality as well as the inequalities it covers in the further computation. This procedure also ensures the termination of our SuperBall approach. Since each available inequality determines a subset of Region($\mathbf{0}$) and the size of Region($\mathbf{0}$) is finite, then there are only a finite number of available inequalities that cannot cover each other.

Assume we have got an inequality $\bar{f} \geq 0$ in SubSection 3.2, and $\bar{f} \geq 0$ can exclude a subset B of points in Region($\mathbf{0}$). To remove the inequality $\bar{f} \geq 0$ as well as the inequalities it covers, it suffices to add the following constraint to the model

$$\sum_{\mathbf{b} \in \text{Region}(\mathbf{0}) \setminus \mathbf{B}} z_{\mathbf{b}} \geq 1.$$

3.4 On the efficiency of the SuperBall approach

The basic SuperBall approach can efficiently find out all available inequalities if the size of the region is smaller than 100. However, many techniques are necessary for speeding up the algorithm if the size of region is larger than 150. Our implementation is able to finish the computation in a few hours if the size of the region does not exceed 280. We also noted that the number of borders affects the complexity significantly.

4 Detailed results

The Sbox of Keccak [BDPA11] admits five input bits and five output bits, so the inequalities involve 10 variables. The size of C is 317 and there are 707 points to be excluded. The largest region is centered at the point $0x1f$, which contains 231 points and 5 border points. We finally obtain 112316 available inequalities. There may have many duplicated inequalities, because they may be computed from different regions. Using Sasaki and Todo's method, we find the smallest set of inequalities in few seconds. There are 26 inequalities in the smallest set.

$12x_0 + 15x_1 + 5x_2 + 19x_3 + 19x_4 + 3x_5 - 6x_6 + 14x_7 - 9x_8 - 4x_9 \geq 0$

$-3x_0 - 10x_1 - 10x_2 + x_3 - 3x_4 + 7x_5 - 10x_6 - 10x_7 + 2x_8 - 8x_9 + 44 \geq 0$

$7x_0 - x_1 + x_2 - x_3 + 7x_4 - 7x_5 - x_6 - x_7 + 6x_8 - x_9 + 5 \geq 0$
$4x_0 + 3x_1 - 12x_2 - 12x_3 + 2x_4 - 12x_5 + 9x_6 - 12x_7 - 8x_8 + 2x_9 + 44 \geq 0$
$x_0 - x_1 + 7x_2 + 7x_3 - x_4 - x_5 + 6x_6 - x_7 - 7x_8 - x_9 + 5 \geq 0$
$-x_0 - 2x_1 + 19x_2 - 34x_3 - 8x_4 + 3x_5 + 32x_6 + 19x_7 + 39x_8 + 7x_9 + 4 \geq 0$
$3x_0 - 12x_1 - 12x_2 + 2x_3 + 4x_4 + 9x_5 - 12x_6 - 8x_7 + 2x_8 - 12x_9 + 44 \geq 0$
$27x_0 - 20x_1 - 3x_2 + 3x_3 - x_4 - 10x_5 + 20x_6 - 2x_7 + 10x_8 + 28x_9 + 6 \geq 0$
$x_0 - 4x_1 + 2x_2 - 11x_3 + 11x_4 + 3x_5 - 7x_6 + 11x_7 - 11x_8 + 9x_9 + 22 \geq 0$
$-12x_0 + 2x_1 + 4x_2 + 3x_3 - 12x_4 - 8x_5 + 2x_6 - 12x_7 + 9x_8 - 12x_9 + 44 \geq 0$
$11x_0 + x_1 - 4x_2 + 2x_3 - 11x_4 + 9x_5 + 3x_6 - 7x_7 + 11x_8 - 11x_9 + 22 \geq 0$
$-10x_0 - 10x_1 + x_2 - 3x_3 - 3x_4 - 10x_5 - 10x_6 + 2x_7 - 8x_8 + 7x_9 + 44 \geq 0$
$-4x_0 - 9x_1 + 20x_2 - x_3 + 2x_4 + 32x_5 + 29x_6 - 19x_7 + 5x_8 + 11x_9 \geq 0$
$2x_0 + 31x_1 - 24x_2 + x_3 - 4x_4 + 29x_5 - 13x_6 + 22x_7 + 3x_8 + 11x_9 + 6 \geq 0$
$-11x_0 - 11x_1 + 3x_2 + 4x_3 + 2x_4 - 11x_5 - 7x_6 + x_7 - 11x_8 + 9x_9 + 40 \geq 0$
$x_0 - 3x_1 - 3x_2 - 10x_3 - 10x_4 + 2x_5 - 8x_6 + 7x_7 - 10x_8 - 10x_9 + 44 \geq 0$
$-x_0 + x_1 - x_2 + 7x_3 + 7x_4 - x_5 - x_6 + 6x_7 - x_8 - 7x_9 + 5 \geq 0$
$8x_0 - 13x_1 - 3x_2 + 32x_3 - x_4 + 8x_5 + 47x_6 + 35x_7 - 31x_8 + 14x_9 \geq 0$
$-x_0 - 4x_1 + 4x_2 + 18x_3 - 19x_4 + 4x_5 - 4x_6 + 19x_7 + 2x_8 + 16x_9 + 8 \geq 0$
$2x_0 + 4x_1 + 3x_2 - 12x_3 - 12x_4 + 2x_5 - 12x_6 + 9x_7 - 12x_8 - 8x_9 + 44 \geq 0$
$-3x_0 - 3x_1 - 10x_2 - 10x_3 + x_4 - 8x_5 + 7x_6 - 10x_7 - 10x_8 + 2x_9 + 44 \geq 0$
$-x_0 + 7x_1 + 7x_2 - x_3 + x_4 + 6x_5 - x_6 - 7x_7 - x_8 - x_9 + 5 \geq 0$
$-10x_0 + x_1 - 3x_2 - 3x_3 - 10x_4 - 10x_5 + 2x_6 - 8x_7 + 7x_8 - 10x_9 + 44 \geq 0$
$-24x_0 + x_1 - 4x_2 + 2x_3 + 31x_4 + 22x_5 + 3x_6 + 11x_7 + 29x_8 - 13x_9 + 6 \geq 0$
$-7x_0 + 7x_1 - 2x_2 + 2x_3 - x_4 - 7x_5 + 7x_6 - x_7 - 5x_8 + 7x_9 + 16 \geq 0$
$7x_0 + 7x_1 - x_2 + x_3 - x_4 - x_5 - 7x_6 - x_7 - x_8 + 6x_9 + 5 \geq 0$

The are 12 variables in the inequalities of APN [BDMW10]. The size of C is 2017 and we need to exclude 2079 points. The largest region is centered at the point $0x2a$, which contains only 183 points, but it has 18 border points. We totally obtain 55478 available inequalities. The smallest subset that describes C contains 145 inequalities and is given below.

$-12x_0 + 4x_1 - 11x_2 - 12x_3 + 10x_4 - x_5 + 12x_6 - 12x_7 - 8x_8 + 2x_9 + 12x_{10} - 4x_{11} + 48 \geq 0$
$-8x_0 + 6x_1 + 8x_2 + 4x_3 - 8x_4 + 8x_5 + 5x_6 + 2x_7 - 7x_8 + 8x_9 + x_{10} + 4x_{11} + 15 \geq 0$
$-8x_0 + 17x_1 - 6x_2 + 17x_3 - 4x_4 - x_5 + 11x_6 + 19x_7 + 18x_8 + 2x_9 + 15x_{10} + 19x_{11} \geq 0$
$6x_0 + 4x_1 + 8x_2 - 2x_3 + 7x_4 + 8x_5 + 8x_6 - 4x_7 - 8x_8 - 8x_9 + 8x_{10} + x_{11} + 14 \geq 0$
$-x_0 + 6x_1 - 6x_2 - 4x_3 - 5x_4 - 6x_5 + 6x_6 - 6x_7 + 2x_8 + 6x_9 + 6x_{10} - 2x_{11} + 24 \geq 0$
$x_0 + 10x_1 + 11x_2 - 12x_3 - 6x_4 + 2x_5 - 11x_6 - 12x_7 - 12x_8 + 2x_9 + 6x_{10} - 12x_{11} + 53 \geq 0$
$-6x_0 - 6x_1 - 7x_2 - x_3 - 6x_4 - 6x_5 - 4x_6 + 7x_7 - 5x_8 + 6x_9 + 3x_{10} - 2x_{11} + 36 \geq 0$
$2x_0 - 12x_1 - 10x_2 + 12x_3 - 12x_4 - 2x_5 + 10x_6 - 6x_7 - 11x_8 + 12x_9 + x_{10} - 6x_{11} + 47 \geq 0$
$-4x_0 - 4x_1 - 3x_2 + 4x_3 + 3x_4 + x_5 + 2x_6 - 2x_7 + 4x_8 + 2x_9 - 4x_{10} - 4x_{11} + 17 \geq 0$
$4x_0 - 3x_1 + 3x_2 + 4x_3 + 4x_4 - 4x_5 + 2x_6 - 3x_7 + x_8 + 3x_9 + 3x_{10} - 2x_{11} + 8 \geq 0$
$2x_0 - 4x_1 - 4x_2 + 4x_3 + 4x_4 - x_5 + 3x_6 + 2x_7 + 3x_8 - 4x_9 - 4x_{10} + 4x_{11} + 13 \geq 0$
$12x_0 + 8x_1 - 16x_2 - 4x_3 + 16x_4 - x_5 - 8x_6 - 15x_7 - 14x_8 + 2x_9 - 16x_{10} - 16x_{11} + 74 \geq 0$
$6x_0 - 6x_1 - 5x_2 + 6x_3 - 4x_4 + 6x_5 - 4x_6 - 5x_7 + 6x_8 + 2x_9 - 2x_{10} + x_{11} + 20 \geq 0$
$-8x_0 + 24x_1 - 23x_2 + 16x_3 - 20x_4 - 8x_5 - 24x_6 - 24x_7 - 22x_8 + 2x_9 + 4x_{10} - x_{11} + 106 \geq 0$
$6x_0 + 10x_1 - 6x_2 - 10x_3 + 12x_4 + 12x_5 + 12x_6 + 11x_7 - 11x_8 + 2x_9 - x_{10} - 2x_{11} + 18 \geq 0$
$2x_0 - 8x_1 + 10x_2 + 10x_3 + 10x_4 + 3x_5 - 7x_6 - x_7 - 9x_8 - 3x_9 + 10x_{10} - 10x_{11} + 28 \geq 0$

$$x_0 - 2x_1 + 18x_2 - 6x_3 - 14x_4 - 8x_5 + 20x_6 + 30x_7 + 29x_8 + 28x_9 + 30x_{10} + 12x_{11} \geq 0$$
$$-9x_0 + 6x_1 - 9x_2 + 6x_3 + 8x_4 - 3x_5 - 8x_6 + 9x_7 + 8x_8 + 3x_9 - x_{10} - x_{11} + 22 \geq 0$$
$$-2x_0 - 4x_1 + 4x_2 - x_3 - 3x_4 - 4x_5 - 2x_6 - 3x_7 - 4x_8 + 4x_9 + 4x_{10} + 4x_{11} + 19 \geq 0$$
$$-6x_0 + 6x_1 + x_2 - 7x_3 - 7x_4 - 6x_5 - 5x_6 - 4x_7 - 7x_8 + 2x_9 - 3x_{10} - 7x_{11} + 45 \geq 0$$
$$-x_0 + 2x_1 - 3x_2 + 4x_3 - 2x_4 + 4x_5 + 4x_6 + 4x_7 - 4x_8 + 4x_9 - 4x_{10} - 2x_{11} + 12 \geq 0$$
$$-24x_0 - 12x_1 - 22x_2 - 12x_3 + 23x_4 - 2x_5 + 8x_6 - 23x_7 - 20x_8 - x_9 + 16x_{10} + 4x_{11} + 92 \geq 0$$
$$-5x_0 - 4x_1 - 5x_2 - 4x_3 - 5x_4 - 2x_5 - 6x_6 + 6x_7 - x_8 + 2x_9 - 5x_{10} + 5x_{11} + 31 \geq 0$$
$$-3x_0 + 3x_1 + 3x_2 - 3x_3 + x_4 - 3x_5 - 3x_6 - x_7 + x_8 + 3x_9 + 2x_{10} - 3x_{11} + 13 \geq 0$$
$$4x_0 + 6x_1 - 8x_2 + 8x_3 + 8x_4 - 2x_5 + 7x_6 + 4x_7 - 7x_8 + 8x_9 - x_{10} - 8x_{11} + 18 \geq 0$$
$$-12x_0 + 12x_1 + 12x_2 - 10x_3 + 12x_4 + 2x_5 - 8x_6 + 11x_7 + 4x_8 + 4x_9 + 12x_{10} + x_{11} + 18 \geq 0$$
$$17x_0 + 17x_1 + 11x_2 + 17x_3 + 17x_4 + 3x_5 - 14x_6 - 5x_7 - 14x_8 - x_9 - 6x_{10} - x_{11} + 24 \geq 0$$
$$-13x_0 + 8x_1 - 4x_2 + 8x_3 + 12x_4 + 9x_5 - 12x_6 + 11x_7 + 12x_8 - 5x_9 + x_{10} + 2x_{11} + 21 \geq 0$$
$$-6x_1 - 6x_2 + 6x_3 - 4x_4 + x_5 + 6x_6 + 5x_7 + 2x_8 - 6x_9 + 2x_{10} - 6x_{11} + 22 \geq 0$$
$$-7x_0 - x_1 + 8x_2 + 4x_3 + 6x_4 - 8x_5 + 8x_6 - 4x_7 - 8x_8 - 8x_9 - 8x_{10} - 2x_{11} + 38 \geq 0$$
$$4x_0 - 12x_1 - 14x_2 - 12x_3 - 16x_4 - 4x_5 - 15x_6 + 16x_7 - 16x_8 - 4x_9 - x_{10} + 2x_{11} + 78 \geq 0$$
$$6x_0 + 2x_1 + 5x_2 + 2x_3 - 6x_4 - 6x_5 + 4x_6 + 6x_7 - 5x_8 + 6x_9 + x_{10} + 4x_{11} + 11 \geq 0$$
$$13x_0 - 16x_1 + 12x_2 - 16x_3 + 19x_4 - 19x_5 - 7x_6 + 19x_7 + 6x_8 + x_9 - 3x_{10} + x_{11} + 42 \geq 0$$
$$x_0 - 16x_1 - 8x_2 + 14x_3 + 15x_4 + 16x_5 - 16x_6 + 12x_7 - 15x_8 + 2x_9 + 8x_{10} + 4x_{11} + 39 \geq 0$$
$$-12x_0 + 10x_1 + 12x_2 + 12x_3 - 12x_4 + 2x_5 + 11x_6 - 10x_7 - 6x_8 + 2x_9 - x_{10} - 6x_{11} + 35 \geq 0$$
$$-2x_0 + 10x_1 - 9x_2 - 4x_3 + 10x_4 - x_5 - 10x_6 - 10x_7 + 4x_8 - 10x_9 + 10x_{10} + 6x_{11} + 36 \geq 0$$
$$-11x_0 - 11x_1 + 9x_2 - 11x_3 + 7x_4 + 11x_5 + 11x_6 + 11x_7 - 3x_8 + 4x_9 + x_{10} - 2x_{11} + 27 \geq 0$$
$$-6x_0 - 4x_1 - 6x_2 - 2x_3 - 6x_4 - x_5 - 6x_6 + 3x_7 + 3x_8 + 4x_9 + 6x_{10} - 6x_{11} + 31 \geq 0$$
$$17x_0 + 26x_1 + 26x_2 + 20x_3 + 16x_4 + 26x_5 - 8x_6 - 5x_7 + 9x_8 + 6x_9 - 5x_{10} - 8x_{11} \geq 0$$
$$10x_0 - 4x_1 - 10x_2 - 6x_3 - 3x_4 - 3x_5 - 10x_6 + 5x_7 + 5x_8 - 6x_9 - 10x_{10} - 10x_{11} + 52 \geq 0$$
$$-4x_0 - 8x_1 - 8x_2 - 7x_3 + 8x_4 - x_5 + 7x_6 + 4x_7 - 6x_8 - 8x_9 + 2x_{10} + 8x_{11} + 34 \geq 0$$
$$-2x_0 + x_1 + 4x_2 - 4x_3 - 4x_4 + 3x_5 - 2x_6 - 3x_7 - 4x_8 - 3x_9 - 3x_{10} - 4x_{11} + 25 \geq 0$$
$$-7x_0 + 7x_1 + 3x_2 - 4x_3 + x_4 + 7x_5 + 2x_6 - 7x_7 + 3x_8 - 5x_9 + 4x_{10} - 5x_{11} + 21 \geq 0$$
$$-18x_0 + 10x_1 + 17x_2 + 10x_3 + 18x_4 - 18x_5 + 18x_6 + 6x_7 - 4x_8 + 4x_9 + 2x_{10} - x_{11} + 23 \geq 0$$
$$2x_0 - 6x_1 + 6x_2 + 6x_3 - 4x_4 + 2x_5 + 5x_6 + 4x_7 - 6x_8 + 6x_9 - x_{10} + 6x_{11} + 11 \geq 0$$
$$-x_0 - 6x_1 - 6x_2 + 4x_3 - 5x_4 - 6x_5 + 5x_6 - 4x_7 + 2x_8 + 6x_9 + 6x_{10} + 2x_{11} + 22 \geq 0$$
$$-x_0 + 10x_1 + 11x_2 - 12x_3 - 6x_4 - 2x_5 - 12x_6 - 12x_7 - 11x_8 - 2x_9 + 6x_{10} - 12x_{11} + 58 \geq 0$$
$$8x_0 + 8x_1 + 7x_2 - 2x_3 + 8x_4 - 8x_5 + 6x_6 - 8x_7 + 7x_8 - 2x_9 - x_{10} - 2x_{11} + 15 \geq 0$$
$$9x_0 - 6x_1 - 9x_2 - 6x_3 + 8x_4 + 3x_5 - 8x_6 + 9x_7 + 8x_8 + 3x_9 + x_{10} + x_{11} + 20 \geq 0$$
$$8x_0 - 7x_1 + 7x_2 - 7x_3 + 6x_4 + 2x_5 - 8x_6 + 8x_7 - 8x_8 + 2x_9 + x_{10} + 2x_{11} + 22 \geq 0$$
$$5x_0 + 2x_1 - 5x_2 + 3x_3 - 5x_4 + x_5 - 5x_6 + 2x_7 + 5x_8 + 3x_9 + 5x_{10} - 5x_{11} + 15 \geq 0$$
$$-14x_0 - 9x_1 + 12x_2 + 14x_3 + 3x_4 + 14x_5 + 12x_6 - 11x_7 + 10x_8 + 4x_9 - 4x_{10} - 2x_{11} + 26 \geq 0$$
$$13x_0 + 16x_1 + 12x_2 + 19x_3 + 6x_4 + 19x_5 - 13x_6 - 11x_7 + 11x_8 + 3x_9 + 2x_{10} + 7x_{11} + 5 \geq 0$$
$$4x_0 + 6x_1 + 7x_2 + 5x_3 + 2x_4 + 7x_5 - 5x_6 + x_7 + 3x_8 - 5x_9 - 5x_{10} + 5x_{11} + 8 \geq 0$$
$$2x_0 + 6x_1 + 6x_2 - 6x_3 - 6x_4 - 2x_5 + 5x_6 + 4x_7 - 5x_8 - 6x_9 - x_{10} - 6x_{11} + 26 \geq 0$$
$$12x_0 + 12x_1 + 11x_2 - 2x_3 + 12x_4 - 12x_5 + 11x_6 - 6x_7 + 10x_8 + 6x_9 + 2x_{10} + x_{11} + 8 \geq 0$$
$$6x_0 - 2x_1 + 5x_2 - 2x_3 - 6x_4 + 6x_5 + 4x_6 + 6x_7 - 5x_8 - 6x_9 + x_{10} - 4x_{11} + 19 \geq 0$$
$$-6x_0 + 20x_1 - 16x_2 + 14x_3 + 19x_4 - x_5 + 4x_6 - 20x_7 + 20x_8 + 2x_9 - 6x_{10} + 20x_{11} + 29 \geq 0$$
$$10x_0 - 7x_1 + 10x_2 - 10x_3 - 2x_4 + 8x_5 - 10x_6 - 10x_7 + 9x_8 - x_9 + 3x_{10} + 3x_{11} + 30 \geq 0$$
$$-8x_0 + 20x_1 - 23x_2 + 24x_3 - 16x_4 + 4x_5 - 22x_6 - 24x_7 - 24x_8 - 2x_9 + 8x_{10} - x_{11} + 96 \geq 0$$
$$-10x_0 + 10x_1 + 9x_2 - 8x_3 + 2x_4 + 10x_5 + 9x_6 - 8x_7 + 7x_8 + 3x_9 - 3x_{10} + x_{11} + 19 \geq 0$$

$$x_0 - 6x_1 - 6x_2 - 4x_3 - 3x_4 + 6x_5 + x_6 + 6x_7 - 6x_8 + 6x_9 - 6x_{10} - 3x_{11} + 28 \geq 0$$
$$-5x_0 + 5x_1 + 2x_2 - 5x_3 - 4x_4 + 3x_5 - 2x_6 - 5x_7 + 5x_8 + x_9 - 5x_{10} + 5x_{11} + 21 \geq 0$$
$$x_0 + 10x_1 - 2x_2 - 7x_3 + 9x_4 - 10x_5 - 10x_6 + 10x_7 - 9x_8 - 3x_9 + 8x_{10} - 3x_{11} + 34 \geq 0$$
$$-x_0 + 16x_1 - 15x_2 + 16x_3 - 16x_4 + 4x_5 + 4x_6 - 12x_7 - 14x_8 - 16x_9 + 4x_{10} - 2x_{11} + 60 \geq 0$$
$$-x_0 - 7x_1 - 8x_2 - 8x_3 - 4x_4 + 2x_5 - 6x_6 - 8x_7 + 8x_8 - 8x_9 - 8x_{10} - 4x_{11} + 54 \geq 0$$
$$11x_0 - 3x_1 - 7x_2 + 11x_3 - 9x_4 - 11x_5 - 11x_6 - 10x_7 - 11x_8 - x_9 + 2x_{10} + 4x_{11} + 52 \geq 0$$
$$3x_0 - x_1 + 3x_2 - x_3 + 3x_4 + 3x_5 + 3x_6 - 3x_7 - 3x_8 + 2x_9 - 2x_{10} + 7 \geq 0$$
$$6x_0 + 5x_1 - 4x_2 - 5x_3 - 6x_4 - 6x_5 - 5x_6 - 6x_7 + 6x_8 + x_9 + 2x_{10} + 2x_{11} + 26 \geq 0$$
$$-x_0 + 16x_1 - 8x_2 - 14x_3 + 15x_4 - 16x_5 - 16x_6 + 12x_7 - 15x_8 + 2x_9 + 8x_{10} + 4x_{11} + 54 \geq 0$$
$$x_0 + 9x_1 + 9x_2 - 9x_3 - 9x_4 + 9x_5 + 9x_6 - 6x_7 + 8x_8 - 3x_9 - 3x_{10} + x_{11} + 21 \geq 0$$
$$x_0 - 18x_1 - 6x_2 - 18x_3 - 6x_4 + 2x_5 + 17x_6 + 16x_7 + 16x_8 - 2x_9 + 12x_{10} + 18x_{11} + 32 \geq 0$$
$$-2x_0 + 2x_1 + 2x_2 + 2x_3 - 2x_4 - 2x_5 + x_7 - 2x_8 - 2x_9 + x_{10} + 2x_{11} + 8 \geq 0$$
$$-x_0 - 10x_1 + 9x_2 + 7x_3 - 2x_4 + 3x_5 - 10x_6 - 8x_7 - 10x_8 + 3x_9 - 8x_{10} + 10x_{11} + 39 \geq 0$$
$$4x_0 - 4x_1 - 4x_2 - 4x_3 + 4x_4 + x_5 - 4x_6 - 3x_7 - 4x_8 - x_9 - 4x_{10} + x_{11} + 24 \geq 0$$
$$4x_0 - 3x_1 + 3x_2 + 4x_3 + 4x_4 - 4x_5 + x_6 - 4x_7 + 2x_8 - 3x_9 - 2x_{10} + 3x_{11} + 12 \geq 0$$
$$-16x_0 - 14x_1 + 12x_2 - 16x_3 - 8x_4 - 8x_5 + 15x_6 - 12x_7 - 16x_8 - 4x_9 - x_{10} + 2x_{11} + 79 \geq 0$$
$$-12x_0 - 12x_1 + 9x_2 - 12x_3 + 11x_4 + 6x_5 - 12x_6 - 12x_7 - 6x_8 - x_9 + 3x_{10} + x_{11} + 55 \geq 0$$
$$-3x_0 - 2x_1 + x_2 - 2x_3 - 3x_4 + 3x_5 - x_6 + 3x_7 - 2x_8 + 3x_9 - x_{10} - 3x_{11} + 14 \geq 0$$
$$10x_0 + 14x_1 + 20x_2 + 15x_3 + 20x_4 + 20x_5 - 8x_6 + 5x_7 + 10x_8 - x_9 - 8x_{10} - 3x_{11} \geq 0$$
$$x_0 - 6x_1 - 8x_2 + 8x_3 + 7x_4 + 8x_5 - 8x_6 + 8x_7 - 7x_8 + 2x_9 - 2x_{10} + 2x_{11} + 23 \geq 0$$
$$-x_0 - 10x_1 + 12x_2 + 12x_3 - 6x_4 - 2x_5 - 11x_6 - 6x_7 - 12x_8 + 2x_9 - 6x_{10} + 12x_{11} + 42 \geq 0$$
$$5x_0 - 5x_1 - 4x_2 + 5x_3 + 5x_4 - x_5 + 2x_6 - 2x_7 + 5x_8 - 3x_9 + 5x_{10} - 5x_{11} + 15 \geq 0$$
$$-6x_0 + 4x_1 - 5x_2 - 4x_3 - 6x_4 + 6x_5 - 6x_6 - 5x_7 + 6x_8 + 2x_9 + 2x_{10} - x_{11} + 27 \geq 0$$
$$x_0 + 2x_1 - 4x_2 - 4x_3 - 4x_4 - 4x_5 + 3x_6 - 4x_7 + 4x_8 - 4x_9 - 4x_{10} + 2x_{11} + 24 \geq 0$$
$$x_0 - 7x_1 - 2x_2 + 10x_3 + 9x_4 + 10x_5 - 10x_6 + 10x_7 - 9x_8 + 3x_9 + 8x_{10} - 3x_{11} + 21 \geq 0$$
$$-2x_0 - 5x_1 - 5x_2 + 6x_3 + 4x_4 - 2x_5 - 6x_6 - 4x_7 + 6x_8 + 6x_9 - 6x_{10} + x_{11} + 24 \geq 0$$
$$-x_0 - 15x_1 - 16x_2 - 15x_3 - 14x_4 + 4x_5 - 12x_6 + 16x_7 - 15x_8 - 4x_9 + 4x_{10} - 2x_{11} + 78 \geq 0$$
$$22x_0 + 2x_1 + 19x_2 + 5x_3 + 20x_4 + 6x_5 - 16x_6 + 15x_7 - 20x_8 + 3x_9 + 20x_{10} - 5x_{11} + 19 \geq 0$$
$$x_0 - 22x_1 + 16x_2 - 22x_3 + 24x_4 - 4x_5 + 20x_6 + 24x_7 + 23x_8 + 2x_9 - 8x_{10} - 8x_{11} + 40 \geq 0$$
$$3x_0 - 7x_1 + 2x_2 + 7x_3 - 8x_4 + 3x_5 + 10x_6 + 8x_7 - 10x_8 - 10x_9 + x_{10} - 10x_{11} + 35 \geq 0$$
$$8x_0 + 4x_1 - 10x_2 + 4x_3 - 10x_4 - x_5 + 2x_6 + 9x_7 + 10x_8 + 6x_9 - 8x_{10} + 10x_{11} + 19 \geq 0$$
$$-x_0 + 4x_1 - 7x_2 + 8x_3 + 6x_4 - 4x_5 + 6x_6 + 8x_7 - 8x_8 - 8x_9 - 2x_{10} + 8x_{11} + 22 \geq 0$$
$$-2x_0 + 8x_1 + 6x_2 - 7x_3 - 8x_4 + 2x_5 - 7x_6 + 7x_7 - 8x_8 - 2x_9 - 8x_{10} - x_{11} + 35 \geq 0$$
$$16x_0 + 4x_1 - 14x_2 + 12x_3 + 15x_4 + 2x_5 + 12x_6 - 15x_7 - 8x_8 - x_9 - 12x_{10} + 8x_{11} + 34 \geq 0$$
$$-5x_0 - 3x_1 - x_2 - 3x_3 - 5x_4 + 5x_5 - 6x_6 + 6x_7 - 4x_8 - 5x_9 - 2x_{10} + 5x_{11} + 28 \geq 0$$
$$10x_0 - 5x_1 - 10x_2 - 5x_3 - 3x_4 - 3x_5 - 6x_6 + 10x_7 + 4x_8 - 5x_9 + 10x_{10} + 10x_{11} + 27 \geq 0$$
$$-x_0 - 16x_1 - 15x_2 - 16x_3 - 14x_4 - 4x_5 - 12x_6 + 16x_7 - 16x_8 - 4x_9 - 4x_{10} - 2x_{11} + 88 \geq 0$$
$$x_0 - 8x_1 + 6x_2 - 8x_3 - 8x_4 - 2x_5 + 7x_6 - 8x_7 + 8x_8 + 2x_9 - 2x_{10} - 8x_{11} + 36 \geq 0$$
$$3x_0 - x_1 + 11x_2 + 3x_3 + 21x_4 + 2x_5 + 18x_6 + 21x_7 + 19x_8 + 21x_9 - 10x_{10} - 10x_{11} \geq 0$$
$$2x_0 - 10x_1 - 9x_2 + 4x_3 + 10x_4 - x_5 - 10x_6 - 10x_7 + 4x_8 + 10x_9 - 10x_{10} - 6x_{11} + 46 \geq 0$$
$$7x_0 - 2x_1 + 7x_2 - 7x_3 - 7x_4 - x_5 - 5x_6 - 4x_7 + 6x_8 + 3x_9 - 5x_{10} - 5x_{11} + 29 \geq 0$$
$$-2x_0 + 15x_1 - 5x_2 + 17x_3 + 13x_4 - 4x_5 + 12x_6 - 3x_7 + 17x_8 - 4x_9 + 14x_{10} + 17x_{11} + 1 \geq 0$$
$$x_0 + 7x_1 - 3x_2 - 5x_3 - 6x_4 + 7x_5 + 7x_6 - 7x_7 + 3x_8 + 7x_9 - 7x_{10} - 2x_{11} + 23 \geq 0$$
$$-x_0 + 6x_1 + 6x_2 + 6x_3 - 3x_4 + 3x_5 - x_6 + 6x_7 + 5x_8 - 6x_9 + 6x_{10} - 6x_{11} + 11 \geq 0$$
$$x_0 + 3x_1 - 3x_2 - 3x_3 + 3x_4 - x_5 + 2x_6 + 3x_7 + 3x_8 - 3x_9 - 3x_{10} + 3x_{11} + 10 \geq 0$$

$$-x_0+2x_1+5x_2+2x_3-6x_4-4x_5-6x_6+6x_7+5x_8+6x_9-6x_{10}-6x_{11}+23\geq 0$$
$$-2x_0-12x_1+12x_2+12x_3-10x_4+12x_5+12x_6-8x_7+11x_8-4x_9-4x_{10}+x_{11}+28\geq 0$$
$$16x_0-15x_1+15x_2-15x_3+12x_4-14x_5-2x_6+16x_7-4x_8+4x_9+x_{10}-4x_{11}+38\geq 0$$
$$-7x_0+5x_1-7x_2+5x_3-x_4+x_5-2x_6+7x_7+7x_8-2x_9+7x_{10}+7x_{11}+12\geq 0$$
$$16x_0+16x_1-15x_2-4x_3+14x_4+x_5+8x_6-15x_7-12x_8+2x_9-16x_{10}-8x_{11}+54\geq 0$$
$$-x_0-4x_1-4x_2+2x_3-4x_4-4x_5+3x_6-4x_7+4x_8-4x_9-4x_{10}+2x_{11}+25\geq 0$$
$$-3x_0-7x_1-7x_2+7x_3+4x_4+5x_5-7x_6-2x_7-7x_8-x_9-7x_{10}-7x_{11}+41\geq 0$$
$$-3x_0+24x_1+17x_2+24x_3+24x_4-3x_5+24x_6+7x_7+21x_8-2x_9-8x_{10}-8x_{11}\geq 0$$
$$2x_0-7x_1+6x_2+8x_3-8x_4+2x_5-8x_6+8x_7-8x_8+2x_9-8x_{10}-x_{11}+32\geq 0$$
$$+4x_1-4x_2-4x_3-2x_4+x_5+4x_6+3x_7+4x_8-4x_9+2x_{10}-4x_{11}+14\geq 0$$
$$4x_0+3x_1+4x_2+3x_3-x_4-4x_5-4x_6+2x_7-4x_8-4x_9-2x_{10}-4x_{11}+19\geq 0$$
$$16x_0+12x_1+16x_2+16x_3-15x_4+x_5-8x_6-14x_7+15x_8-2x_9+4x_{10}-8x_{11}+31\geq 0$$
$$-x_0-8x_1-7x_2-8x_3-7x_4-2x_5+8x_6-8x_7-6x_8-8x_9+2x_{10}-2x_{11}+49\geq 0$$
$$-x_0-7x_1-8x_2-8x_3-4x_4+2x_5-6x_6-7x_7+8x_8+8x_9+8x_{10}-4x_{11}+37\geq 0$$
$$-6x_0+4x_1-5x_2+4x_3+x_4+2x_5-5x_6+6x_7+5x_8-2x_9-5x_{10}-5x_{11}+22\geq 0$$
$$2x_0+13x_1-6x_2-13x_3-14x_4-2x_5+14x_6+6x_7-7x_8+8x_9+x_{10}+14x_{11}+28\geq 0$$
$$-6x_0-6x_1+4x_2+6x_3-5x_4-2x_5-6x_6-4x_7+2x_8+x_9+6x_{10}+6x_{11}+23\geq 0$$
$$-10x_0-9x_1+8x_2+10x_3+x_4+10x_5+7x_6-10x_7+8x_8-3x_9+2x_{10}+3x_{11}+22\geq 0$$
$$9x_0+9x_1-9x_2-3x_3-8x_4+9x_5-6x_6-6x_7-9x_8+3x_9+x_{10}+x_{11}+32\geq 0$$
$$3x_0-4x_1+3x_2+3x_3-2x_4-3x_5-x_6-3x_7-3x_8-3x_9-2x_{10}+4x_{11}+17\geq 0$$
$$8x_0+20x_1-20x_2+20x_3-12x_4-2x_5+4x_6-18x_7-19x_8-20x_9-4x_{10}-x_{11}+76\geq 0$$
$$-x_0-8x_1-13x_2+8x_3+4x_4-14x_5+14x_6+13x_7-14x_8+6x_9+2x_{10}-10x_{11}+46\geq 0$$
$$12x_0-12x_1+10x_2-8x_3-11x_4+x_5-12x_6-10x_7+12x_8-2x_9-4x_{10}+4x_{11}+47\geq 0$$
$$3x_0-9x_1-12x_2-12x_3+11x_4-x_5+12x_6-6x_7+12x_8+x_9+6x_{10}+12x_{11}+28\geq 0$$
$$-4x_0-2x_1-20x_2-3x_3-20x_4+5x_5+16x_6+15x_7+17x_8+18x_9-5x_{10}+20x_{11}+34\geq 0$$
$$14x_0+8x_1+6x_2+7x_3+9x_4+14x_5+4x_6+5x_7-7x_8-8x_9+4x_{10}+8x_{11}+1\geq 0$$
$$-5x_0-5x_1+2x_2+5x_3-4x_4-3x_5-5x_6-2x_7+5x_8-x_9-5x_{10}-5x_{11}+30\geq 0$$
$$x_0+16x_1+14x_2-16x_3-15x_4-16x_5-12x_6+15x_7+8x_8-4x_9-8x_{10}-2x_{11}+57\geq 0$$
$$-x_0+5x_1+6x_2-6x_3+6x_4-2x_5-4x_6-6x_7-5x_8-2x_9-6x_{10}+6x_{11}+26\geq 0$$
$$-x_0-6x_1-5x_2+3x_3+5x_4-x_5-6x_6-6x_7+6x_8-6x_9+6x_{10}-3x_{11}+28\geq 0$$
$$-2x_0+5x_1+2x_2+x_3-5x_4-5x_5-3x_6-4x_7-5x_8+5x_9+5x_{10}-5x_{11}+24\geq 0$$
$$-2x_0-7x_1-10x_2-6x_3-3x_4+10x_5+10x_6-4x_7+5x_8-10x_9+10x_{10}+10x_{11}+32\geq 0$$
$$2x_0+6x_1-5x_2-5x_3+4x_4-2x_5-6x_6-6x_7+6x_8+6x_9-6x_{10}+x_{11}+24\geq 0$$
$$-x_0+19x_1-18x_2+20x_3-20x_4+2x_5-6x_6-20x_7-12x_8-14x_9-8x_{10}+2x_{11}+79\geq 0$$
$$-15x_0+12x_1+3x_2+15x_3-12x_4-4x_5+13x_6-11x_7-10x_8-12x_9-2x_{10}-5x_{11}+56\geq 0$$
$$x_0-14x_1+16x_2+14x_3-15x_4-16x_5-12x_6+15x_7+8x_8-4x_9-8x_{10}+2x_{11}+53\geq 0$$
$$-9x_0-13x_1+11x_2+13x_3+13x_4+2x_5-13x_6+8x_7-4x_8+x_9+13x_{10}-5x_{11}+31\geq 0$$
$$-2x_0-5x_1+4x_2-5x_3-5x_4-x_5-2x_6+6x_7+5x_8-6x_9+6x_{10}-6x_{11}+26\geq 0$$
$$-x_0+10x_1-15x_2+11x_3+8x_4+3x_5+15x_6+5x_7+16x_8+6x_9+16x_{10}+16x_{11}\geq 0$$

References

[AST+17] Ahmed Abdelkhalek, Yu Sasaki, Yosuke Todo, Mohamed Tolba, and Amr M. Youssef. Milp modeling for (large) s-boxes to optimize probability of differential characteristics. *IACR Trans. Symmetric Cryptol.*, 2017(4):99–129, 2017.

[BC20] Christina Boura and Daniel Coggia. Efficient milp modelings for sboxes and linear layers of spn ciphers. *IACR Trans. Symmetric Cryptol.*, 2020(3):327–361, 2020.

[BDMW10] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An apn permutation in dimension six. *Finite Fields: theory and applications*, 42:33–42, 2010.

[BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The keccak reference, version 3.0. In *https://keccak.team/keccak.html*, 2011.

[Dil09] John Dillon. Apn polynomials: An update. *Invited talk at Fq9, the 9th International Conference on Finite Fields and Applications*, July 2009.

[GO21] LLC Gurobi Optimization. Gurobi optimizer reference manual, 2021.

[SHW+14a] Siwei Sun, Lei Hu, Meiqin Wang, Peng Wang, Kexin Qiao, Xiaoshuang Ma, Danping Shi, Ling Song, and Kai Fu. Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. Cryptology ePrint Archive, Report 2014/747, 2014. `https://ia.cr/2014/747`.

[SHW+14b] Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, des(l) and other bit-oriented block ciphers. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014*, pages 158–178, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[ST17] Yu Sasaki and Yosuke Todo. New algorithm for modeling s-box in milp based differential and division trail search. In Pooya Farshim and Emil Simion, editors, *Innovative Security Solutions for Information Technology and Communications*, pages 150–165, Cham, 2017. Springer International Publishing.