UDC 003.26:512.5

Systems of Linear Restrictions Over a Finite Field

Oleh Kurinnyi[1, a]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Institute of Physics and Technology*

Abstract

This paper considers the problem of recovering an unknown vector based on partial information presented in the form of certain linear dependencies. Such problem is an alternative to the standard one of solving a system of polynomial equations over a finite field, which arises in the context of algebraic cryptanalysis of stream ciphers, and it models a situation when it's not possible to formulate specific equations with an unknown vector, but certain restrictions on linear dependencies with this vector. To formalize such linear dependencies, the notation of the system of linear restrictions over a finite field is introduced, and the problem of recovering the unknown vector is replaced by the problem of solving the system of linear restrictions over a finite field. In this paper, we researched some properties of this problem using its equivalent forms and important partial cases.

Keywords: system of linear restrictions, algebraic cryptanalysis, finite field, stream ciphers.

1. Introduction

Standard models of algebraic cryptanalysis search dependencies between plaintexts, ciphertexts and keys in the form of the system of polynomial equations over a finite field [1, 2, 3]. We can consider an alternative task in which only restrictions on possible values of some dependencies with unknown parameters are known. The study of such problem is expedient, since there are many methods that help to obtain partial information about the intermediate values of some parameters during the encryption process. These methods can indicate that certain dependencies with unknown parameters cannot take some finite set of values. Such information can be obtained from a side channel or from the weaknesses of the cryptosystem implementation. Given this, the problem of recovering an unknown vector based on partial information presented in the form of certain linear dependencies arises.

In this paper, we propose a formalization of this problem by introducing the notation of a system of linear restrictions over a finite field, prove a number of properties of such systems and give equivalent forms of this problem. At the end of paper, we research the solution set properties of systems with zero right-hand sides.

The obtained theoretical results can be used in algebraic cryptanalysis of stream ciphers and cryptosystems based on linear codes [4].

2. Basic terms and notations

Let's define the linear restriction and the system of linear restrictions with analogy to the linear equation and the system of linear equations.

Definition 1. *The linear restriction over a field* $\mathbb{F}_{2^k}$ is an expression of the form

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \neq a_0, \qquad (1)$$

where $a_i \in \mathbb{F}_{2^k}$ for $i = \overline{0, n}$, $x_i \in \mathbb{F}_{2^k}$ for $i = \overline{1, n}$.

If we denote $a = (a_1, a_2, \ldots, a_n)$, then we can rewrite the linear restriction as $(a, x) \neq a_0$, where $(a, x) = \sum_{i=1}^{n} a_ix_i$ is a dot product of a and x. In fact, the linear restriction means that $a_1x_1 + a_2x_2 + \ldots + a_nx_n \in \mathbb{F}_{2^k} \setminus \{0\}$. Depending on the context, we'll also call the linear restriction the vector $(a_1, a_2, \ldots, a_n, a_0)$ for $a_0 \neq 0$ and the vector $(a_1, a_2, \ldots, a_n)$ for $a_0 = 0$. Also, when $(a, x_0) = 0$ holds for $x_0 \in \mathbb{F}_{2^k}^n$ we will say that a vector *a restricts* vector x_0 or that these vectors are *orthogonal.*

Definition 2. *The solution of the linear restriction* is a vector $x_0 \in \mathbb{F}_{2^k}^n$ such that $(a, x_0) \neq a_0$. *The solution set of the linear restriction* is a set of vectors $\{x \in \mathbb{F}_{2^k}^n \mid (a, x) \neq a_0\}$. If solution sets of two restrictions are equal, we will say that these linear restrictions are *equivalent.*

[a] ol.kurinnoy@gmail.com

Let's find out what elementary operations with linear restrictions we can perform to get equivalent restrictions.

Claim 1. *The solution set of the linear restriction doesn't change while moving terms from one side of the restriction to another, as well as multiplying both sides by a non-zero constant.*

Proof. Consider the linear restriction of the form (1). Denote sets $D_0 = \{x \in \mathbb{F}_{2^k}^n \mid (a, x) \neq a_0\}$, $D'_0 = \mathbb{F}_{2^k}^n \setminus D_0$, i.e. D'_0 consists of all $x \in \mathbb{F}_{2^k}^n$ such that $(a, x) = a_0$.

Let's form another linear restriction

$$a_2x_2 + \ldots + a_nx_n \neq a_1x_1 + a_0.$$

Similarly, we define sets D_1 and D'_1. The set D'_1 consists of all $x \in \mathbb{F}_{2^k}^n$ such that

$$a_2x_2 + \ldots + a_nx_n = a_1x_1 + a_0.$$

After moving term a_1x_1 to the left side of equation, we get

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = a_0.$$

It follows that $D'_1 = D'_0$ and therefore $D_1 = D_0$, because sets D_0, D'_0 and D_1, D'_1 aren't intersected. Proof of the constant multiplying part is the same. ■

Also we can calculate the cardinality of the linear restrictions solution set exactly.

Claim 2. *For the linear restriction*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \neq a_0$$

over a finite field $\mathbb{F}_{2^k}$ the cardinality of the solution set is equal to $2^{kn} - 2^{k(n-1)}$.

Proof. Consider the corresponding linear equation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = a_0$ and D' – its solution set. The left side of this equation is a linear function with respect to variables $x_1, x_2, \ldots, x_n$, so the expression $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ takes each value of $\mathbb{F}_{2^k}$ the same number of times, namely $|D'| = 2^{k(n-1)}$. So, the linear restriction solution set $D = \mathbb{F}_{2^k}^n \setminus D'$ has the cardinality $|D| = |\mathbb{F}_{2^k}^n| - |D'| = 2^{kn} - 2^{k(n-1)}$. ■

Definition 3. *The system of linear restrictions over a field* $\mathbb{F}_{2^k}$ is a system of expressions of the form

$$\begin{cases} a_1^{(1)}x_1 + a_2^{(1)}x_2 + \ldots + a_n^{(1)}x_n \neq a_0^{(1)}, \\ a_1^{(2)}x_1 + a_2^{(2)}x_2 + \ldots + a_n^{(2)}x_n \neq a_0^{(2)}, \\ \ldots \\ a_1^{(m)}x_1 + a_2^{(m)}x_2 + \ldots + a_n^{(m)}x_n \neq a_0^{(m)}, \end{cases} \tag{2}$$

where $a_i^{(j)} \in \mathbb{F}_{2^k}$ for $i = \overline{0,n}, j = \overline{1,m}$, $x_t \in \mathbb{F}_{2^k}$ for $t = \overline{1,n}$, and $m > 1$.

Shortly we can denote $a^{(j)} = (a_1^{(j)}, a_2^{(j)}, \ldots, a_n^{(j)})$ and rewrite the system (2) as:

$$\begin{cases} (a^{(1)}, x) \neq a_0^{(1)}, \\ (a^{(2)}, x) \neq a_0^{(2)}, \\ \ldots \\ (a^{(m)}, x) \neq a_0^{(m)}. \end{cases}$$

Also we can even more short notation: if A is $(m \times n)$-matrix over a $\mathbb{F}_{2^k}$ of the form

$$A = \begin{pmatrix} a^{(1)} \\ a^{(2)} \\ \ldots \\ a^{(m)} \end{pmatrix} = \left\{a_i^{(j)}\right\}_{i=\overline{1,n}}^{j=\overline{1,m}}$$

and a_0 is $(m \times 1)$-vector of the form

$$a_0 = \begin{pmatrix} a_0^{(1)} \\ a_0^{(2)} \\ \ldots \\ a_0^{(m)} \end{pmatrix}$$

then the system (2) takes from $A \cdot x \neq a_0$, where symbol «$\neq$» is used in untypical context and stands for «not equal in all components».

Similarly to the linear restriction, we can define the solution of the system of linear restrictions.

Definition 4. *The solution of the system of linear restrictions* is a vector $x_0 \in \mathbb{F}_{2^k}^n$ such that $A \cdot x \neq a_0$. *The solution set of the system of linear restrictions* is a set of vectors

$$\{x \in \mathbb{F}_{2^k}^n \mid A \cdot x \neq a_0\} = D_1 \cap D_2 \cap \ldots \cap D_m, \tag{3}$$

where D_j – the solution set of corresponding linear restriction in the system, $j \in \overline{1,m}$. If solution sets of two systems are equal, we will say that these systems are *equivalent.*

Claim 3. *The solution set of the system of linear restrictions doesn't change while moving terms from one side to another in any restriction of the system, as well as multiplying both sides of any restriction by a non-zero constant.*

Proof. This statement follows directly from claim 1 and formula (3). ■

3. Equivalent forms of the problem of solving the system of linear restrictions over a finite field

Let's consider several problems equivalent to the system of linear restrictions. These alternative problems provide other ways of characterizing the original problem, thus expanding the set of available methods that can be applied to it. Consider the following tasks.

1) Checking the polynomial, which specifies a certain multilinear form, for the identical equality to zero over a finite field.
2) Solving a system of quadratic equations of a certain type over a finite field.
3) Checking whether a polynomial belongs to an ideal (of polynomial ring) of a certain type.

We'll say that the polynomial $f \in \mathbb{F}_{2^k}[x_1, \dots, x_n]$ is *identically equal to zero* over $\mathbb{F}_{2^k}$ if for all $x \in \mathbb{F}_{2^k}^n$ holds $f(x) = 0$.

Claim 4. *The system of linear restrictions $A \cdot x \neq a_0$ over a field $\mathbb{F}_{2^k}$ has a solution if and only if the polynomial*

$$F(x) = \prod_{i=1}^{m} \left((a^{(i)}, x) + a_0^{(i)} \right) \tag{4}$$

isn't identically equal to zero over $\mathbb{F}_{2^k}$.

Proof. We will prove this fact in the following form: the system of linear restrictions $A \cdot x \neq a_0$ has no solutions if and only if $F(x) \equiv 0$. Since proving the necessity and sufficiency of this criterion are quite similar, we will not consider these two cases separately. The nonexistence of solutions of the system (2) is equivalent to the fact that for every $x \in \mathbb{F}_{2^k}^n$ at least one restriction is not satisfied, namely, it turns into equality. We can write it in this way:

$$\forall x \in \mathbb{F}_{2^k}^n \ \exists i \in \overline{1, m} : (a^{(i)}, x) + a_0^{(i)} = 0.$$

Consider a polynomial which is equal to the product of the left sides of all linear restrictions (see formula (4)). For every given value of x there will be a factor, that is equal to 0, so the entire product will turn into zero. Thus, for all $x \in \mathbb{F}_{2^k}^n$ holds $F(x) = 0$. And this, in fact, means that the polynomial F over a field $\mathbb{F}_{2^k}$ is identically to zero because it converges to zero at every possible input. ■

Having this criterion, the idea arises to analytically check whether the polynomial $F(x)$ is identically equal to zero. Unfortunately, when opening the parentheses, an exponential number of terms can potentially appear – we are dealing with a polynomial of degree m and n variables, which generally contains C_{n+m-1}^{n-1} terms. Moreover, even opening the parentheses does not always provide an answer to this question, since in a finite field there are polynomials with nonzero coefficients that are identically equal to zero over this field, for example, the polynomial $x^2 + x$ over the field $\mathbb{F}_2$.

There are a number of works dedicated to the study of the PIT problem (short for Polynomial Identity Testing) [5, 6]. In these papers, probabilistic and even deterministic polynomial algorithms for solving partial cases of PIT are presented, including arithmetic schemes of the $\Pi\Sigma$ type. But these results are not applicable to the above-described problem of checking the identical equality to zero over a finite field, since in these results «the identical equality to zero» means the equality of all coefficients of the polynomial in the canonical form to zero. Therefore, all methods of solving this task such as replacing different monomials with monomials of a higher degree from one variable cannot be transferred to the context of our problem.

Now let's consider the method of replacing the relation «$\neq$» with the usual equality using a transformation called the *«Rabinovitch trick»* [7]. It uses the following idea: let introduce the new variable $\gamma \in \mathbb{F}_{2^k}$ and replace the restriction $x \neq 0$, $x \in \mathbb{F}_{2^k}$, by equality $1 + \gamma \cdot x = 0$. We will show that with such a replacement, the solution set of the initial system of restrictions remains unchanged up to the introduced artificial variables.

Claim 5. *The solution set of the system of linear restrictions (2) is equal to the solution set of the system equations*

$$\begin{cases} 1 + \gamma_1 \cdot \left((a^{(1)}, x) + a_0^{(1)} \right) = 0, \\ 1 + \gamma_2 \cdot \left((a^{(2)}, x) + a_0^{(2)} \right) = 0, \\ \dots \\ 1 + \gamma_m \cdot \left((a^{(m)}, x) + a_0^{(m)} \right) = 0 \end{cases} \tag{5}$$

up to artificial variables $\gamma_1, \gamma_2, \dots, \gamma_m$, where $\gamma_j \in \mathbb{F}_{2^k}$, $j \in \overline{1, m}$.

Proof. Let D be the solution set of the system of restrictions (2), which consists of vectors of size n, and R is the solution set of the system of equations (5), which consists of vectors of size $n + m$. Let's agree that each vector from R first contains $y_1, y_2, \dots, y_n$, and then $y_{n+1} = \gamma_1, y_{n+2} = \gamma_2, \dots, y_{n+m} = \gamma_m$. We will also denote $y_{1:n}$ – a vector of first n components of the vector y.

Now we'll show that if $x \in D$, then exists $y \in R$ such that $y_{1:n} = x$. So, if x is a solution of system of linear restrictions (2), then exists the following set of elements $z_1, z_2, \dots, z_m$, where $z_j \neq 0$, $j \in \overline{1, m}$, that satisfy equalities

$$\begin{cases} (a^{(1)}, x) + a_0^{(1)} = z_1, \\ (a^{(2)}, x) + a_0^{(2)} = z_2, \\ \dots \\ (a^{(m)}, x) + a_0^{(m)} = z_m. \end{cases}$$

We substitute all z_i for $i = \overline{1,m}$ into the system of equations:

$$\begin{cases} 1 + \gamma_1 \cdot z_1 = 0, \\ 1 + \gamma_2 \cdot z_2 = 0, \\ \dots \\ 1 + \gamma_m \cdot z_m = 0. \end{cases}$$

If we put $\gamma_j = (z_j)^{-1}$, $j = \overline{1,m}$, we'll get get the solution y, which belongs to the set R and whose first n components coincide with the vector x.

Let's show that if $y \in R$, then $y_{1:n} \in D$. If y is a solution of the system of equations, then

$$\begin{cases} 1 + \gamma_{n+1} \cdot \left((a^{(1)}, y_{1:n}) + a_0^{(1)}\right) = 0, \\ 1 + \gamma_{n+2} \cdot \left((a^{(2)}, y_{1:n}) + a_0^{(2)}\right) = 0, \\ \dots \\ 1 + \gamma_{n+m} \cdot \left((a^{(m)}, y_{1:n}) + a_0^{(m)}\right) = 0. \end{cases}$$

It follows that $(a^{(j)}, y_{1:n}) + a_0^{(j)}$ is not equal to zero for $j = \overline{1,m}$, because in the case when for some number $1 \le i \le m$ the expression $(a^{(i)}, y_{1:n}) + a_0^{(i)}$ turns into zero, we have the contradiction. And this, in turn, means that $y_{1:n} \in D$. ■

The resulting system is a partial case of the MQ problem (short for Multivariate Quadratic polynomial), which consists in solving the system of quadratic equations over a finite field. It is known that the MQ problem is $\mathcal{NP}$-complete [8].

Let's move on to the last equivalent form of the original problem. Consider the lemma that characterizes all polynomials of one variable, that identically equal to zero over a finite field $\mathbb{F}_{2^k}$.

Lemma 1. *Polynomial $F \in \mathbb{F}_{2^k}[x]$ is identically equal to zero over $\mathbb{F}_{2^k}$ if and only if this polynomial can be represented in the form*

$$F(x) = G(x) \cdot (x^{2^k} + x),$$

where $G \in \mathbb{F}_{2^k}[x]$. Such representation is equivalent to $(x^{2^k} + x) | F(x)$.

Proof. *Necessity.* Let $F(x) = 0$ for every $x \in \mathbb{F}_{2^k}$. Then by Bezout's theorem $(x + g) \mid F(x)$ for every $g \in \mathbb{F}_{2^k}$, therefore the product of these polynomials also divides $F(x)$, but the product $\prod_{g \in \mathbb{F}_{2^k}} (x + g)$, in turn, is equal to $x^{2^k} + x$ in a finite field, therefore $(x^{2^k} + x) | F(x)$.

Sufficiency. Let $(x^{2^k} + x) \mid F(x)$, namely $F(x) = G(x) \cdot (x^{2^k} + x)$ for some $G \in \mathbb{F}_{2^k}[x]$. Since $x^{2^k} + x = 0$ for all $x \in \mathbb{F}_{2^k}$, then $F(x)$ also equals to zero for $x \in \mathbb{F}_{2^k}$. ■

Theorem 1. *Polynomial $F \in \mathbb{F}_{2^k}[x_1, \dots, x_n]$ is identically equal to zero over $\mathbb{F}_{2^k}$ if and only if this polynomial can be represented in the form*

$$F(x_1, \dots, x_n) = \sum_{i=0}^{n} G_1(x_1, \dots, x_n) \cdot (x_i^{2^k} + x_i), \tag{6}$$

where $G_1, \dots, G_n \in \mathbb{F}_{2^k}[x_1, \dots, x_n]$.

Proof. *Necessity.* We will prove the statement of the theorem by induction on the number of variables. The basis of the induction follows from lemma 1. Assume that the required statement holds for n variables, that is, any polynomial $H \in \mathbb{F}_{2^k}[x_1, \dots, x_n]$ such that $H(x_1, \dots, x_n) \equiv 0$, can be represented in the required form. Consider the polynomial of $(n + 1)$ variables $F \in \mathbb{F}_{2^k}[x_1, \dots, x_{n+1}]$ for which $H(x_1, \dots, x_{n+1}) \equiv 0$ (note that F cannot contain constants in the canonical representation, because otherwise the condition of identical equality to zero would not be satisfied). We can represent this polynomial in the following way:

$$F(x_1, \dots, x_{n+1}) =$$
$$= \sum_{i=1}^{n+1} \sum_{l=0}^{\deg F} x_i^l H^{(i,l)}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}),$$

where each of the polynomials $H^{(i,l)}$ does not depend on variable x_i, i.e. depends on n variables, $i = \overline{1, n+1}$, $l = \overline{0, \deg F}$. Such representation can be obtained using a «greedy» algorithm, which for each variable x_i, $1 \le i \le n+1$, and l, $0 \le l \le \deg F$, performs the following steps.

1) Selects in F all monomials, which contains x_i^l, i.e. such monomials divisible by x_i^l, but not divisible by x_i^{l+1}.
2) Groups all such monomials and put x_i^l over the parentheses. The polynomial, that remains in parentheses, is denoted by the variable $H^{(i,l)}$. This polynomial does not depend on the variable x_i, because the monomial, that includes this variable, was put out the brackets.

For each of these polynomials, we can apply induction assumptions, that is, represent them in the form:

$$H^{(i,l)}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}) =$$
$$= \sum_{1 \le j \le n+1, j \ne i} R_j^{(i,l)} \cdot (x_j^{2^k} + x_j),$$

where each of the polynomials $R_j^{(i,l)}$ depends on the variables $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}$. We can put $R_i^{(i,l)} \equiv 0$ and rewrite $H^{(i,l)}$:

$$H^{(i,l)}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1}) =$$
$$= \sum_{j=1}^{n+1} R_j^{(i,l)} \cdot (x_j^{2^k} + x_j).$$

So, the polynomial $F(x_1, \ldots, x_{n+1})$ can be rewritten in the following way:

$$F(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{n+1} \sum_{l=0}^{\deg F} x_i^l \sum_{j=1}^{n+1} R_j^{(i,l)} \cdot (x_j^{2^k} + x_j).$$

Now we can enter x_i^l under the sum over variable j and swap the sums over j and l, since these summation indices are independent from each other. After replacing $Q_j^{(i)} = \sum_{l=0}^{\deg F} x_i^l R_j^{(i,l)}$, polynomial $F(x_1, \ldots, x_{n+1})$ will have the following form:

$$F(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} Q_j^{(i)} \cdot (x_j^{2^l} + x_j).$$

Since the summation indices in these two sums are independent of each other, we change the order of summation and subtract $(x_j^{2^k} + x_j)$ into the first sum:

$$F(x_1, \ldots, x_{n+1}) = \sum_{j=1} (x_j^{2^k} + x_j) \sum_{i=1}^{n+1} Q_j^i.$$

For convenience, we denote $G_j = \sum_{i=1}^{n+1} Q_j^{(i)}$ and rewriting $F(x_1, \ldots, x_n)$ in new notations give us required equality (6).

Sufficiency. Suppose that the polynomial F can be represented in in the required form. Since $x_j^{2^k} + x_j = 0$ for all $1 \leq j \leq n$, then each term in the representation is zero for an arbitrary set of values of the variables $x_1, \ldots, x_n$, so the polynomial F identically equals to zero. ■

Corollary 1. *The polynomial $F \in \mathbb{F}_{2^k}[x_1, \ldots, x_n]$ is identically equal to zero over the field $\mathbb{F}_{2^k}$ if and only if F belongs to the ideal*

$$I = (x_1^{2^k} + x_1, \ldots, x_n^{2^k} + x_n).$$

Consider the quotient ring $\mathbb{F}_{2^k}[x_1, \ldots, x_n]/I$, then there exists a canonical homomorphism

$$\pi : \mathbb{F}_{2^k}[x_1, \ldots, x_n] \to \mathbb{F}_{2^k}[x_1, \ldots, x_n]/I,$$

where $\pi(F) = F \bmod I$ denotes the remainder of dividing the polynomial F by the system of polynomials that generate the ideal I. Under this canonical homomorphism, all polynomials in $\mathbb{F}_{2^k}[x_1, \ldots, x_n]$, that identically equal to zero, will get into the adjacency class of the zero polynomial in $\mathbb{F}_{2^k}[x_1, \ldots, x_n]/I$. Thus, the procedure of checking the ideal I membership can be reduced to finding the image of the polynomial F under the mapping π, i.e. finding the remainder of the division of F by the system of polynomials $(x_1^{2^k} + x_1, \ldots, x_n^{2^k} + x_n)$. This remainder of the division will be zero if and only if the polynomial F identically equals to zero over $\mathbb{F}_{2^k}$. Note, that if the polynomial F would be represented in the canonical form (that is, as the arithmetic circuit of the $\Sigma\Pi$ type), then it would be possible to perform this division efficiently (in fact, by the standard algorithm of «column division» [9]), but in our case, the polynomial is represented as the arithmetic circuit of the $\Pi\Sigma$ type.

4. Properties of the systems of linear restrictions with zero right sides

Suppose that one of the solutions of the system of linear restrictions with zero right-hand sides is known. The question arises whether in this case it is possible to say something about other solutions or whether it is even possible to restore some of them.

Lemma 2. *Let $z = (z_1, \ldots, z_n)$ is a solution of the system of linear restrictions $A \cdot x \neq \overline{0}$ over a field $\mathbb{F}_{2^k}$. Then $z' = (bz_1, bz_2, \ldots, bz_n)$, where $b \in \mathbb{F}_{2^k} \setminus \{0\}$, is also solution of this system.*

Proof. Let z be the solution of the system of linear restrictions, then

$$\begin{cases} a_1^{(1)} z_1 + a_2^{(1)} z_2 + \ldots + a_n^{(1)} z_n = y_1, \\ a_1^{(2)} z_1 + a_2^{(2)} z_2 + \ldots + a_n^{(2)} z_n = y_2, \\ \qquad \ldots \\ a_1^{(m)} z_1 + a_2^{(m)} z_2 + \ldots + a_n^{(m)} z_n = y_m, \end{cases} \tag{7}$$

where $y_1, y_2, \ldots, y_m \in \mathbb{F}_{2^k} \setminus \{0\}$.

Let's multiply the left and right sides of all equations by the element $b \in \mathbb{F}_{2^k} \setminus \{0\}$ and replace $z_i' = bz_i$, $i = \overline{1,n}$, and $y_j' = by_j$, $j = \overline{1,m}$. After these operations we get the following system

$$\begin{cases} a_1^{(1)} z_1' + a_2^{(1)} z_2' + \ldots + a_n^{(1)} z_n' = y_1', \\ a_1^{(2)} z_1' + a_2^{(2)} z_2' + \ldots + a_n^{(2)} z_n' = y_2', \\ \qquad \ldots \\ a_1^{(m)} z_1' + a_2^{(m)} z_2' + \ldots + a_n^{(m)} z_n' = y_m'. \end{cases} \tag{8}$$

Since $b \neq 0$, the new variables $y_j' \neq 0$, $j = \overline{1,m}$. Therefore, $(z_1, z_2, \ldots, z_n)$ – also the solution of the initial system $A \cdot x \neq \overline{0}$. ■

So, other solutions can be reconstructed from a known solution. Let's formulate a theorem that describes the structure of the solution set of the system of linear restrictions with zero right-hand sides.

Claim 6. *Let $D \subseteq \mathbb{F}_{2^k}^n$ – the solution set of the system of linear restrictions $A \cdot x \neq \overline{0}$ over a finite field $\mathbb{F}_{2^k}$, then $|D|$ is divisible by $2^k - 1$.*

Proof. Consider a binary relation on the solution set D of the system of linear restrictions: two vectors $a, b \in D$ are in the relation $\sim$ if there is an element $c \in \mathbb{F}_{2^k} \setminus \{0\}$ such that

$$(a_1, a_2, \ldots, a_n) = (cb_1, cb_2, \ldots, cb_n).$$

Such a relation will be called a *proportionality relation*, and the vectors belonging to this relation will be called *proportional*.

We will show that the relation $\sim$ is an equivalence relation.

- *Reflexivity.* The property $\forall z \in D : z \sim z$ always holds, since we can choose $c = 1$.
- *Symmetry.* We need to check the statement

  $$\forall x, y \in D : x \sim y \Rightarrow y \sim x.$$

  If $x \sim y$, then there exists $c \in \mathbb{F}_{2^k} \setminus \{0\}$ such that $x_i = cy_i$, $i \in \overline{1, n}$. Since $c \in \mathbb{F}_{2^k} \setminus \{0\}$, then $c^{-1} \in \mathbb{F}_{2^k} \setminus \{0\}$ exists, so $y_i = c^{-1}x_i$, $i = \overline{1, n}$. In this case,

  $$(y_1, y_2, \ldots, y_n) = (c^{-1}x_1, c^{-1}x_2, \ldots, c^{-1}x_n),$$

  which means that $y \sim x$.
- *Transitivity.* We need to check the statement

  $$\forall x, y, z \in D : x \sim y, y \sim z \Rightarrow x \sim z.$$

  Suppose $x \sim y$ and $y \sim z$, then there exist $c_1, c_2 \in \mathbb{F}_{2^k} \setminus \{0\}$ such that $x_i = c_1 y_i$ and $y_i = c_2 z_i$, $i = \overline{1, n}$. We substitute $y_i = c_2 z_i$. $i = \overline{1, n}$, into the condition $x \sim y$ and get $x_i = c_1 c_2 z_i$, $i = \overline{1, n}$. Since $c_1 c_2 \in \mathbb{F}_{2^k} \setminus \{0\}$, then $x \sim z$.

The equivalence relation on the set D defines the partition of this set into equivalence classes: $D = D_1 \cup D_2 \cup \ldots \cup D_s$, where $D_i \cap D_j = \varnothing$ for $i \neq j$, and s is the number of equivalence classes. Thus, any two elements of the same class D_i, $i \in \overline{1, s}$, are in the relation $\sim$, and any two elements of different classes D_i and D_j, where $i \neq j$, are not in the equivalence relation.

Each of the equivalence classes consists of $2^k - 1$ vectors. This can be verified by considering the set

$$\{z \in \mathbb{F}_{2^k}^n \mid z = b \cdot z', b \in \mathbb{F}_{2^k} \setminus \{0\}\},$$

where z – any solution that generates this equivalence class, and ensuring that this set contains exactly 2^{k-1} elements. Since all classes do not intersect with each other, then

$$|D| = s \cdot (2^k - 1)$$

which completes the proof. ■

5. Conclusions

In this article, we formalize the problem of recovering an unknown vector based on partial information presented in the form of linear dependencies by introducing the notation of the system of linear restrictions over a finite binary field. Then we found several equivalent problems such as checking a multilinear form for identical equality to zero over a finite field, solving a system of quadratic equations of a certain form over a finite field and the problem of checking the ideal membership for polynomial (for specific ideals), which connect systems of linear restrictions with existing mathematical problems. As an important partial case, the properties of systems of linear restrictions with zero right-hand sides are formulated and proved. The obtained theoretical results make possible to cover some partial cases of systems of linear restrictions and gained more insights about their structure.

References

[1] G. Bard, *Algebraic Cryptanalysis.* Springer Science+Business Media, LLC, 1 ed., 2009. ISBN: 978-0-387-88756-2.

[2] A. Joux, *Algorithmic Cryptanalysis.* Chapman & Hall, 1 ed., 2009. ISBN: 9781420070026.

[3] A. Alekseychuk, “Algebraic immunity of vectorial boolean functions and boolean groebner bases,” *Theoretical and Applied Cybersecurity*, vol. 2, pp. 10–14, June 2020.

[4] A. Menezes, S. Vanstone, and P. van Oorschot, *Handbook of Applied Cryptography.* CRC Press, 1 ed., 1996. ISBN: 0-8493-8523-7.

[5] M. Agrawal and S. Biswas, “Primality and identity testing via chinese remaindering,” *Journal of the ACM*, vol. 50, pp. 429–443, July 2003.

[6] A. Shpilka and A. Yehudayoff, “Arithmetic circuits: A survey of recent results and open questions,” *Foundations and Trends in Theoretical Computer Science*, vol. 5, pp. 207–388, March 2010.

[7] S. Arora and B. Barak, *Computational Complexity: A Modern Approach.* Cambridge University Press, 1 ed., 2009. ISBN: 978-0521424264.

[8] A. S. Fraenkel and Y. Yesha, “Complexity of solving algebraic equations,” *Inf. Process. Lett.*, vol. 10, pp. 178–179, 1980.

[9] D. A. Cox, J. B. Little, and D. O’Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, 4 ed., 2015. ISBN: 978-3319167206.