

Article

The Development of Suitable Inequalities and Their Application to Systems of Logical Equations

Dostonjon Numonjonovich Barotov ^{1,*}, Ruziboy Numonjonovich Barotov ², Vladimir Soloviev ¹,
Vadim Feklin ¹, Dilshod Muzafarov ², Trusunboy Ergashboev ² and Khudoyberdi Egamov ³

¹ Department of Data Analysis and Machine Learning, Financial University under the Government of the Russian Federation, 109456 Moscow, Russia; vsoloviev@fa.ru (V.S.); vfeclin@fa.ru (V.F.)

² Department of Mathematical Analysis, Khujand State University, 1 Mavlonbekova, Khujand 735700, Tajikistan; ruzmet.tj@mail.ru (R.N.B.); muzafarov.dilshod@gmail.com (D.M.); tergashboev@mail.ru (T.E.)

³ Department of Higher and Applied Mathematics, Khujand State University, 1 Mavlonbekova, Khujand 735700, Tajikistan; egamov1951@gmail.com

* Correspondence: dnbarotov@fa.ru

Abstract: In this paper, two not-difficult inequalities are invented and proved in detail, which adequately describe the behavior of discrete logical functions $xor(x_1, x_2, \dots, x_n)$ and $and(x_1, x_2, \dots, x_n)$. Based on these proven inequalities, infinitely differentiable extensions of the logical functions $xor(x_1, x_2, \dots, x_n)$ and $and(x_1, x_2, \dots, x_n)$ were defined for the entire $\mathbb{R}^n$. These suitable extensions were applied to systems of logical equations. Specifically, the system of m logical equations in a constructive way without adding any equations (not field equations and no others) is transformed in $\mathbb{R}^n$ first into an equivalent system of m smooth rational equations ($SmSRE$) so that the solution of $SmSRE$ can be reduced to the problem minimization of the objective function, and any numerical optimization methods can be applied since the objective function will be infinitely differentiable. Again, we transformed $SmSRE$ into an equivalent system of m polynomial equations ($SmPE$). This means that any symbolic methods for solving polynomial systems can be used to solve and analyze an equivalent $SmPE$. The equivalence of these systems has been proved in detail. Based on these proofs and results, in the next paper, we plan to study the practical applicability of numerical optimization methods for $SmSRE$ and symbolic methods for $SmPE$.

Keywords: inequalities; proof of inequalities; application of inequalities; Zhegalkin polynomials; logical operations; systems of logical equations; algebraic cryptanalysis; approximation; numerical optimization; system of polynomial equations

MSC: 26D15; 26D20; 97H30; 26D07; 06E30; 03G05; 65H10; 90C09; 90C23; 90C26



Citation: Barotov, D.N.; Barotov, R.N.; Soloviev, V.; Feklin, V.; Muzafarov, D.; Ergashboev, T.; Egamov, K. The Development of Suitable Inequalities and Their Application to Systems of Logical Equations. *Mathematics* **2022**, *10*, 1851. <https://doi.org/10.3390/math10111851>

Academic Editor: Milica Klaricic Bakula

Received: 27 April 2022

Accepted: 26 May 2022

Published: 27 May 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

For many years, systems of logical equations have been an important area of research. The solution of logical equations penetrates into many areas of modern science, such as logical design, biology, grammar, chemistry, law, medicine, spectroscopy, and graph theory [1]. Numerous problems in operations research may be reduced to the solution of a system of logical equations. A striking example is the problem of a coalition game of n people with a dominance relation between different strategies [2]. Solutions of logical equations also serve as an important tool in the processing of pseudo-Boolean equations and inequalities and associated problems of integer linear programming [2].

Another important and promising area in which the solution of a system of logical equations is used is algebraic cryptanalysis. For a specific cipher, algebraic cryptanalysis consists of two stages: transforming the cipher into a system of polynomial equations (usually over a Boolean ring) and solving the resulting system of polynomial equations [3].

One of the first successful applications of solving a system of logical equations in a cryptographic problem was demonstrated in [4]. Therefore, many new directions and algorithms for solving systems of logical equations are being developed and adapted [5–11]. One such direction is the transformation to the real continuous domain, since the real continuous domain is a richer area to work with since it includes many well-developed methods and algorithms. The essence of this direction lies in the fact that the system of logical equations is transformed into a system in a real domain and the solution is sought in a real continuous domain. The transformed system is reducible to a numerical optimization problem. It enables the application, analysis, and combination of techniques such as the steepest descent algorithm, Newton's method, and the coordinate descent algorithm [11–18].

Very recently, in [17,18], an interesting idea was proposed, namely, based on the proofs of simple inequalities, an arbitrary system of logical equations was transformed into the corresponding unique system of polylinear–polynomial equations in a unit n -dimensional cube K_n . In K_n , the equivalence of systems of logical and polylinear–polynomial equations was shown after adding one equation of a special form to the system. In K_n , the solution of a system of polylinear–polynomial equations was reduced to the problem of optimizing a polylinear objective function. The authors found that, according to the system of equations, the composed polylinear objective function does not have a local extremum either inside, or on the edges, or on the faces of K_n . It takes the minimum value at the vertices of K_n .

In this paper, we approached this issue from the point of view of constructively finding a system of m rational (polynomial) equations, which in $\mathbb{R}^n$ is equivalent to a system of m logical equations based on suitable inequalities. Thus, two simple inequalities were constructed and shown in detail. Thanks to the proofs of the transformations of these inequalities into equalities, we have determined (found) suitable smooth (infinitely differentiable) extensions of the discrete logical functions $xor(x_1, x_2, \dots, x_n)$ and $and(x_1, x_2, \dots, x_n)$ relative to the entire domain $\mathbb{R}^n$. These suitable extensions are applied to systems of logical equations. Namely, the system of m logical equations in a constructive way without adding any equations (not field equations and no others) is transformed in $\mathbb{R}^n$ first into an equivalent system of m smooth rational equations so that the solution of the system of m smooth rational equations can be reduced to the problem minimization of the objective function and any numerical optimization methods can be applied since the objective function will be infinitely differentiable. Again, we transformed the system of m smooth rational equations into an equivalent system of m polynomial equations. This means that any symbolic methods for solving polynomial systems can be used to solve and analyze an equivalent system of m polynomial equations. The equivalence of these systems has been proved in detail.

2. A Suitable Inequality for the Logical Operation $xor(x_1, x_2, \dots, x_n)$ and a Proof of Its Necessary Properties

First, we define or recall the necessary notations and formulas for further convenience.

Let $\mathbb{R}^n = \{ (x_1, x_2, \dots, x_n) : x_k \in \mathbb{R} = (-\infty; +\infty), \forall k \in \{1, 2, \dots, n\} \}$ be an n -dimensional real domain.

Let $\mathbb{B}^n = \{ (b_1, b_2, \dots, b_n) : b_k \in \mathbb{B} = \{0, 1\}, \forall k \in \{1, 2, \dots, n\} \}$ be an n -dimensional unit Boolean cube.

Let $\oplus$ be the logical operation xor (addition by mod 2), i.e., $xor(y_1, y_2, \dots, y_n) = y_1 \oplus y_2 \oplus \dots \oplus y_n$, $y_i \in \{0, 1\}$, $\forall i \in \{1, 2, \dots, n\}$. Let $\otimes$ be the logical operation and (logical multiplication), i.e., $and(y_1, y_2, \dots, y_n) = y_1 \otimes y_2 \otimes \dots \otimes y_n$, $y_i \in \{0, 1\}$, $\forall i \in \{1, 2, \dots, n\}$.

In this section, we formulate and prove one inequality that “adequately” describes the behavior of the logical function $xor(x_1, x_2, \dots, x_n)$, and based on this provable inequality, we define a suitable infinitely differentiable extension of the logical function $xor(x_1, x_2, \dots, x_n)$ to the entire domain $\mathbb{R}^n$.

Proposition 1. If $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ and the following is the case:

$$\text{xor}_d(x_1, x_2, \dots, x_n) = \frac{1}{2} - \frac{1}{2} \cdot \prod_{k=1}^n \frac{(2-4x_k)}{1+(1-2x_k)^2},$$

then the following comparisons are true:

- (i) $0 \leq \text{xor}_d(x_1, x_2, \dots, x_n) \leq 1, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$;
- (ii) $\text{xor}_d(x_1, x_2, \dots, x_n) \in \mathbb{B}^1 = \{0, 1\} \Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n$;
- (iii) $\text{xor}_d(x_1, x_2, \dots, x_n) = 0 \Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n$ and $x_1 + x_2 + \dots + x_n$ —even;
- (iv) $\text{xor}_d(x_1, x_2, \dots, x_n) = 1 \Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n$ and $x_1 + x_2 + \dots + x_n$ —odd.

Proof of Proposition 1.

- (i) For any $x \in \mathbb{R}$, $0 \leq (1 - |1 - 2 \cdot x|)^2 \Leftrightarrow 2 \cdot |1 - 2 \cdot x| \leq 1 +$

$$(1 - 2 \cdot x)^2 \Leftrightarrow \frac{|2 - 4 \cdot x|}{1 + (1 - 2 \cdot x)^2} \leq 1 \Leftrightarrow -1 \leq \frac{(2 - 4 \cdot x)}{1 + (1 - 2 \cdot x)^2} \leq 1.$$

It follows from the last inequality that the following is the case.

$$-1 \leq \frac{(2 - 4x_1)}{1 + (1 - 2x_1)^2} \cdot \frac{(2 - 4x_2)}{1 + (1 - 2x_2)^2} \cdot \dots \cdot \frac{(2 - 4x_n)}{1 + (1 - 2x_n)^2} \leq 1, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$$

Alternatively, it is the same as the following.

$$0 \leq \text{xor}_d(x_1, x_2, \dots, x_n) \leq 1, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n;$$

- (ii) First, we prove in the direct direction, if $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$, then the following is the case:

$$x_k \in \mathbb{B}^1, \forall k \in \{1, 2, \dots, n\} \Rightarrow \frac{(2-4x_k)}{1+(1-2x_k)^2} \in \{-1, 1\}, \forall k \in \{1, 2, \dots, n\} \Rightarrow$$

$$-\frac{1}{2} \cdot \frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}$$

or it is the same as the following.

$$\text{xor}_d(x_1, x_2, \dots, x_n) \in \mathbb{B}^1 = \{0, 1\}, \forall (x_1, x_2, \dots, x_n) \in \mathbb{B}^n.$$

Now, we prove in the opposite direction, if $\text{xor}_d(x_1, x_2, \dots, x_n) \in \{0, 1\} \Rightarrow$.

$$\frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} \in \{-1, 1\} \Rightarrow$$

$$\left| \frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} \right| = 1 \Rightarrow \left| \frac{(2-4x_k)}{1+(1-2x_k)^2} \right| = 1,$$

$$\forall k \in \{1, 2, \dots, n\} \Rightarrow x_k \in \mathbb{B}^1, \forall k \in \{1, 2, \dots, n\} \Rightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n;$$

- (iii) First, let us prove in the direct direction, if $\text{xor}_d(x_1, x_2, \dots, x_n) = 0$, then it follows from item (ii) that $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$. Now, note that if $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$, then the following is the case.

$$x_k \in \mathbb{B}^1, \forall k \in \{1, 2, \dots, n\} \Rightarrow \frac{(2-4x_k)}{1+(1-2x_k)^2} = \frac{(2-4x_k)}{1+(\pm 1)^2} = 1 - 2x_k = (-1)^{x_k}, \forall k \in$$

$$\{1, 2, \dots, n\} \Rightarrow 0 = \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} =$$

$$\frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(\pm 1)^2} \cdot \frac{(2-4x_2)}{1+(\pm 1)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(\pm 1)^2} = \frac{1}{2} - \frac{1}{2} \cdot (1 - 2x_1) \cdot (1 - 2x_2) \cdot \dots \cdot (1 - 2x_n)$$

$$= \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1} \cdot (-1)^{x_2} \cdot \dots \cdot (-1)^{x_n} = \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1+x_2+\dots+x_n} \Rightarrow x_1 + x_2 + \dots + x_n \text{—even}.$$

Now we prove in the opposite direction, if $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$ and $x_1 + x_2 + \dots + x_n$ —even, then we have the following.

$$\begin{aligned} 0 &= \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1+x_2+\dots+x_n} = \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1} \cdot (-1)^{x_2} \cdot \dots \cdot (-1)^{x_n} = \\ &= \frac{1}{2} - \frac{1}{2} \cdot (1-2x_1) \cdot (1-2x_2) \cdot \dots \cdot (1-2x_n) = \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(\pm 1)^2} \cdot \frac{(2-4x_2)}{1+(\pm 1)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(\pm 1)^2} \\ &= \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} = \text{xor}_d(x_1, x_2, \dots, x_n); \end{aligned}$$

(iv) This point follows from points (ii) and (iii); for clarity and visibility, we can conduct a separate proof and it is similar to the proof of point (iii).

First, let us prove in the direct direction, if $\text{xor}_d(x_1, x_2, \dots, x_n) = 1$, then it follows from item (ii) that $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$. Now, note that if $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$, then the following obtains.

$$\begin{aligned} x_k \in \mathbb{B}^1, \forall k \in \{1, 2, \dots, n\} &\Rightarrow \frac{(2-4x_k)}{1+(1-2x_k)^2} = \frac{(2-4x_k)}{1+(\pm 1)^2} = 1-2x_k = (-1)^{x_k}, \forall k \in \\ &\{1, 2, \dots, n\} \Rightarrow 1 = \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} = \\ &= \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(\pm 1)^2} \cdot \frac{(2-4x_2)}{1+(\pm 1)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(\pm 1)^2} = \frac{1}{2} - \frac{1}{2} \cdot (1-2x_1) \cdot (1-2x_2) \cdot \dots \cdot (1-2x_n) \\ &= \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1} \cdot (-1)^{x_2} \cdot \dots \cdot (-1)^{x_n} = \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1+x_2+\dots+x_n} \Rightarrow x_1 + x_2 + \dots + x_n \text{—odd}. \end{aligned}$$

Now we prove in the opposite direction, if $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$ и $x_1 + x_2 + \dots + x_n$ —odd, then the following obtains.

$$\begin{aligned} 1 &= \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1+x_2+\dots+x_n} = \frac{1}{2} - \frac{1}{2} \cdot (-1)^{x_1} \cdot (-1)^{x_2} \cdot \dots \cdot (-1)^{x_n} = \\ &= \frac{1}{2} - \frac{1}{2} \cdot (1-2x_1) \cdot (1-2x_2) \cdot \dots \cdot (1-2x_n) = \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(\pm 1)^2} \cdot \frac{(2-4x_2)}{1+(\pm 1)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(\pm 1)^2} \\ &= \frac{1}{2} - \frac{1}{2} \cdot \frac{(2-4x_1)}{1+(1-2x_1)^2} \cdot \frac{(2-4x_2)}{1+(1-2x_2)^2} \cdot \dots \cdot \frac{(2-4x_n)}{1+(1-2x_n)^2} = \text{xor}_d(x_1, x_2, \dots, x_n); \end{aligned}$$

□

Thus, we obtain the following.

$$\forall b \in \{0, 1\}, \text{xor}_d(x_1, x_2, \dots, x_n) = b \Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n \text{ and } \text{xor}(x_1, x_2, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n = b.$$

Based on the last fact, the infinitely differentiable function $\text{xor}_d(x_1, x_2, \dots, x_n)$ can be called a suitable and smoothly continuous extension of the discrete function $\text{xor}(x_1, x_2, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ to the entire domain $\mathbb{R}^n$. Therefore, from the beginning, we decided that the following expression:

$$\frac{1}{2} - \frac{1}{2} \cdot \prod_{k=1}^n \frac{(2-4x_k)}{1+(1-2x_k)^2}$$

would be denoted by $\text{xor}_d(x_1, x_2, \dots, x_n)$.

3. A Suitable Inequality for the Logical Operation $\text{and}(x_1, x_2, \dots, x_n)$ and a Proof of Its Necessary Properties

In this section, we formulate and prove one inequality that “adequately” describes the behavior of the logical function $\text{and}(x_1, x_2, \dots, x_n)$, and based on this provable inequality, we define a suitable infinitely differentiable extension of the logical function $\text{and}(x_1, x_2, \dots, x_n)$ to the entire domain $\mathbb{R}^n$.

Proposition 2. If $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ and the following is the case:

$$\text{and}_d(x_1, x_2, \dots, x_n) = \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2},$$

then the following comparisons are true:

- (i) $0 \leq \text{and}_d(x_1, x_2, \dots, x_n) \leq 1, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$;
- (ii) If $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$, then $\text{and}_d(x_1, x_2, \dots, x_n) \in \mathbb{B}^1 = \{0, 1\}$;
- (iii) $\text{and}_d(x_1, x_2, \dots, x_n) = 0 \Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n \setminus \{(1, 1, \dots, 1)\}$;
- (iv) $\text{and}_d(x_1, x_2, \dots, x_n) = 1 \Leftrightarrow (x_1, x_2, \dots, x_n) = (1, 1, \dots, 1)$.

Proof of Proposition 2.

- (i) The first inequality on the left is obvious, since $0 \leq \frac{x^2}{2x^2 - 2x + 1} \leq 1$ and $\frac{(x^2 - x)^2}{(2x^2 - 2x + 1)^2} \geq 0, \forall x \in \mathbb{R} \Rightarrow \text{and}_d(x_1, x_2, \dots, x_n) =$.

$$\prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} \geq 0, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n.$$

Now, let us prove the second inequality, which is on the right. To perform this, in the process, we also use the inequality between the arithmetic mean and the geometric mean.

$$\begin{aligned} \text{and}_d(x_1, x_2, \dots, x_n) &= \frac{x_1^2}{2x_1^2 - 2x_1 + 1} \cdot \frac{x_2^2}{2x_2^2 - 2x_2 + 1} \cdot \dots \cdot \frac{x_n^2}{2x_n^2 - 2x_n + 1} \\ &+ \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} = \left(\sqrt[n]{\frac{x_1^2}{2x_1^2 - 2x_1 + 1} \cdot \frac{x_2^2}{2x_2^2 - 2x_2 + 1} \cdot \dots \cdot \frac{x_n^2}{2x_n^2 - 2x_n + 1}} \right)^n \\ &+ \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} \leq \left(\frac{1}{n} \cdot \left(\frac{x_1^2}{2x_1^2 - 2x_1 + 1} + \frac{x_2^2}{2x_2^2 - 2x_2 + 1} + \dots + \frac{x_n^2}{2x_n^2 - 2x_n + 1} \right) \right)^n \\ &+ \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} \leq \frac{1}{n} \cdot \left(\frac{x_1^2}{2x_1^2 - 2x_1 + 1} + \frac{x_2^2}{2x_2^2 - 2x_2 + 1} + \dots + \frac{x_n^2}{2x_n^2 - 2x_n + 1} \right) \\ &+ \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} = \frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} \\ &= \frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2 \cdot (2x_k^2 - 2x_k + 1)}{(2x_k^2 - 2x_k + 1)^2} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2 \cdot (2x_k^2 - 2x_k + 1) - x_k^4}{(2x_k^2 - 2x_k + 1)^2} = \\ &\frac{1}{n} \cdot \sum_{k=1}^n \frac{2 \cdot x_k^2 (2x_k^2 - 2x_k + 1) - x_k^4}{(2x_k^2 - 2x_k + 1)^2} = \frac{1}{n} \cdot \sum_{k=1}^n \frac{2 \cdot x_k^2 (2x_k^2 - 2x_k + 1) - x_k^4 - (2x_k^2 - 2x_k + 1)^2}{(2x_k^2 - 2x_k + 1)^2} \\ &+ \frac{1}{n} \cdot \sum_{k=1}^n \frac{(2x_k^2 - 2x_k + 1)^2}{(2x_k^2 - 2x_k + 1)^2} = -\frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - 2x_k + 1)^2}{(2x_k^2 - 2x_k + 1)^2} + \frac{n}{n} \leq 1, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n; \end{aligned}$$

- (ii) If $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$, then the following is obtained.

$$\begin{aligned} x_k \in \mathbb{B}^1, \forall k \in \{1, 2, \dots, n\} &\Rightarrow \frac{x_k^2}{2x_k^2 - 2x_k + 1} = \frac{x_k^2}{2x_k \cdot (x_k - 1) + 1} = \frac{x_k}{0+1} = x_k \in \mathbb{B}^1, \\ \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} &= \frac{(x_k(x_k - 1))^2}{(2x_k(x_k - 1) + 1)^2} = \frac{0^2}{(0+1)^2} = 0 \in \mathbb{B}^1, \forall k \in \{1, 2, \dots, n\} \Rightarrow \\ \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} &+ \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} = \text{and}_d(x_1, x_2, \dots, x_n) \in \mathbb{B}^1; \end{aligned}$$

- (iii) Indeed, the following is the case.

$$\begin{aligned}
and_d(x_1, x_2, \dots, x_n) &= \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} = 0 \Leftrightarrow \\
\begin{cases} \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} = 0 \\ \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} = 0 \end{cases} &\Leftrightarrow \begin{cases} \prod_{k=1}^n x_k^2 = 0 \\ \sum_{k=1}^n (x_k^2 - x_k)^2 = 0 \end{cases} \Leftrightarrow \begin{cases} x_1 \cdot x_2 \cdot \dots \cdot x_n = 0 \\ x_1^2 - x_1 = 0 \\ x_2^2 - x_2 = 0 \\ \dots \dots \dots \\ x_n^2 - x_n = 0 \end{cases} \\
&\Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n \setminus \{(1, 1, \dots, 1)\};
\end{aligned}$$

(iv) Indeed, the following is the case.

$$\begin{aligned}
and_d(x_1, x_2, \dots, x_n) &= \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} = 1 \Leftrightarrow \\
&\left(-1 + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} \right) + \\
&\left(-\frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} \right) = \\
&-\frac{1}{n} \cdot \sum_{k=1}^n \frac{(2x_k^2 - 2x_k + 1)^2}{(2x_k^2 - 2x_k + 1)^2} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2 \cdot (2x_k^2 - 2x_k + 1) - x_k^4}{(2x_k^2 - 2x_k + 1)^2} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2 (2x_k^2 - 2x_k + 1)}{(2x_k^2 - 2x_k + 1)^2} \\
&+ \left(-\frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} \right) = \left(-\frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - 2x_k + 1)^2}{(2x_k^2 - 2x_k + 1)^2} \right) + \\
&\left(-\frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} \right) = 0 \Leftrightarrow \\
&\begin{cases} \sum_{k=1}^n \frac{(x_k^2 - 2x_k + 1)^2}{(2x_k^2 - 2x_k + 1)^2} = 0 \\ -\frac{1}{n} \cdot \sum_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} = 0 \end{cases} \Leftrightarrow \\
\begin{cases} (x_k^2 - 2x_k + 1)^2 = 0, \forall k \in \{1, 2, \dots, n\} \\ \frac{x_i^2}{2x_i^2 - 2x_i + 1} = \frac{x_j^2}{2x_j^2 - 2x_j + 1}, \forall i, j \in \{1, 2, \dots, n\} \end{cases} &\Leftrightarrow (x_1, x_2, \dots, x_n) = (1, 1, \dots, 1);
\end{aligned}$$

□

Thus, we obtain the following:

$$\forall b \in \{0, 1\}, \text{ and } and_d(x_1, x_2, \dots, x_n) = b \Leftrightarrow (x_1, x_2, \dots, x_n) \in \mathbb{B}^n \text{ and } \\
and(x_1, x_2, \dots, x_n) = x_1 \otimes x_2 \otimes \dots \otimes x_n = b.$$

Based on the last fact, the infinitely differentiable function $and_d(x_1, x_2, \dots, x_n)$ can be called a suitable and smoothly continuous extension of the discrete function $and(x_1, x_2, \dots, x_n) = x_1 \otimes x_2 \otimes \dots \otimes x_n$ to the entire domain $\mathbb{R}^n$. Therefore, from the beginning, we decided that the following expression:

$$\prod_{k=1}^n \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2}$$

would be denoted by $and_d(x_1, x_2, \dots, x_n)$.

4. Application of the Developed and Proven Inequalities for the Equivalent Transformation of the System of Logical Equations into the Real Domain $\mathbb{R}^n$

In this section, we apply these contrived and proven inequalities to a system of logical equations. Specifically, we transform the system of m logical equations in $\mathbb{R}^n$ into an equivalent system of m rational equations by using suitable continuations of logical

functions $xor(x_1, x_2, \dots, x_n)$ and $and(x_1, x_2, \dots, x_n)$ without adding any other equations (not field equations of the form $x_k^2 - x_k = 0$ and no other). We prove the equivalence of these systems in great detail.

Consider the following arbitrary system of logical equations:

$$\begin{cases} p_1 = \bigoplus_{(a_1, \dots, a_n) \in \mathbb{B}^n} c_1(a_1, \dots, a_n) \otimes x_1^{a_1} \otimes \dots \otimes x_n^{a_n} = \bigoplus_{c_1(a_1, \dots, a_n)=1} x_1^{a_1} \otimes \dots \otimes x_n^{a_n} = 0 \\ p_2 = \bigoplus_{(a_1, \dots, a_n) \in \mathbb{B}^n} c_2(a_1, \dots, a_n) \otimes x_1^{a_1} \otimes \dots \otimes x_n^{a_n} = \bigoplus_{c_2(a_1, \dots, a_n)=1} x_1^{a_1} \otimes \dots \otimes x_n^{a_n} = 0 \\ p_m = \bigoplus_{(a_1, \dots, a_n) \in \mathbb{B}^n} c_m(a_1, \dots, a_n) \otimes x_1^{a_1} \otimes \dots \otimes x_n^{a_n} = \bigoplus_{c_m(a_1, \dots, a_n)=1} x_1^{a_1} \otimes \dots \otimes x_n^{a_n} = 0 \end{cases} \quad (1)$$

where $x_1, x_2, \dots, x_n \in \{0, 1\}$ —essential variables of the system (1); $\oplus$ —logical operation xor ; $\otimes$ —logical operation and ; $x_i^{a_i} = \begin{cases} 1, & \text{if } a_i = 0 \\ x_i, & \text{if } a_i = 1 \end{cases}$, $p_k = p_k(x_1, \dots, x_n)$ —Zhegalkin polynomial; $c_k(a_1, a_2, \dots, a_n) \in \{0, 1\}$ —coefficient of $x_1^{a_1} \otimes x_2^{a_2} \otimes \dots \otimes x_n^{a_n}$ of polynomial $p_k(x_1, \dots, x_n)$.

Replacing the functions $xor(x_1, x_2, \dots, x_n)$ and $and(x_1, x_2, \dots, x_n)$ with the functions $xor_d(x_1, x_2, \dots, x_n)$ and $and_d(x_1, x_2, \dots, x_n)$ from system (1), we obtain the corresponding smooth transformed system:

$$\begin{cases} f_1(x_1, x_2, \dots, x_n) = \frac{1}{2} - \frac{1}{2} \cdot \prod_{c_1(a_1, a_2, \dots, a_n)=1} \frac{(2 - 4 \cdot and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}))}{1 + (1 - 2 \cdot and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}))^2} = 0 \\ f_2(x_1, x_2, \dots, x_n) = \frac{1}{2} - \frac{1}{2} \cdot \prod_{c_2(a_1, a_2, \dots, a_n)=1} \frac{(2 - 4 \cdot and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}))}{1 + (1 - 2 \cdot and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}))^2} = 0, \\ f_m(x_1, x_2, \dots, x_n) = \frac{1}{2} - \frac{1}{2} \cdot \prod_{c_m(a_1, a_2, \dots, a_n)=1} \frac{(2 - 4 \cdot and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}))}{1 + (1 - 2 \cdot and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}))^2} = 0 \end{cases} \quad (2)$$

where $x_i^{a_i} = \begin{cases} 1, & \text{if } a_i = 0 \\ x_i, & \text{if } a_i = 1 \end{cases}$.

$$and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}) = \prod_{k=1}^n \frac{(x_k^{a_k})^2}{2 \cdot (x_k^{a_k})^2 - 2 \cdot x_k^{a_k} + 1} + \frac{1}{n} \cdot \sum_{k=1}^n \frac{((x_k^{a_k})^2 - x_k^{a_k})^2}{(2 \cdot (x_k^{a_k})^2 - 2 \cdot x_k^{a_k} + 1)^2}.$$

Theorem 1. In $\mathbb{R}^n$, systems (1) and (2) are equivalent in the sense that they have the same solutions.

Proof of Theorem 1. (i) Let $(b_1, b_2, \dots, b_n) \in \mathbb{B}^n$ be an arbitrary solution of system (1). Then, it is obvious that $(b_1^{a_1}, b_2^{a_2}, \dots, b_n^{a_n}) \in \mathbb{B}^n$, $\forall (a_1, a_2, \dots, a_n) \in \mathbb{B}^n \Rightarrow and_d(b_1^{a_1}, b_2^{a_2}, \dots, b_n^{a_n}) \in \mathbb{B}^1$. Now, it follows from Propositions 1 and 2 that $f_k(b_1, b_2, \dots, b_n) = p_k(b_1, b_2, \dots, b_n) = 0$, $\forall k \in \{1, 2, \dots, m\}$ or in other words $(b_1, b_2, \dots, b_n)$ is the solution of system (2). Thus far, we have proved that the set of solutions of system (1) is a subset of the set of solutions of system (2). Conversely, let $(r_1, r_2, \dots, r_n)$ be an arbitrary solution of system (2). This means that $f_k(r_1, r_2, \dots, r_n) = 0$, $\forall k \in \{1, 2, \dots, m\}$. Proposition 1 implies that $and_d(r_1^{a_1}, r_2^{a_2}, \dots, r_n^{a_n}) \in \mathbb{B}^1$, $\forall (a_1, a_2, \dots, a_n) \in \{ (a_1^*, a_2^*, \dots, a_n^*) : c_k(a_1^*, a_2^*, \dots, a_n^*) = 1 \}$ and $\forall k \in \{1, 2, \dots, m\}$. From the fact that any variable is essential for at least one polynomial of system (1) and from Proposition 2, it follows that $(r_1, r_2, \dots, r_n) \in \mathbb{B}^n$. Now, it follows from Propositions 1 and 2 that if $(r_1, r_2, \dots, r_n) \in \mathbb{B}^n$, then $p_k(r_1, r_2, \dots, r_n) = f_k(r_1, r_2, \dots, r_n) = 0$, $\forall k \in \{1, 2, \dots, m\}$ or in other words $(r_1, r_2, \dots, r_n)$ is a solution of system (1). Conversely, we also proved that the set of solutions of system (2) is a subset of solutions of system (1).

Thus, we proved that if at least one system has a solution, then their sets of solutions are equal, or in other words, they are equivalent.

(ii.a) Let system (1) have no solution. Let us prove that, in this case system, (2) also has no solution. From contradiction, let $(r_1, r_2, \dots, r_n)$ be the solution of the system (2).

This means that $f_k(r_1, r_2, \dots, r_n) = 0, \forall k \in \{1, 2, \dots, m\}$. Proposition 1 implies that $and_d(r_1^{a_1}, r_2^{a_2}, \dots, r_n^{a_n}) \in \mathbb{B}^1, \forall (a_1, a_2, \dots, a_n) \in \{(a_1^*, a_2^*, \dots, a_n^*) : c_k(a_1^*, a_2^*, \dots, a_n^*) = 1\}$ and $\forall k \in \{1, 2, \dots, m\}$. From the fact that any variable is essential for at least one polynomial of system (1) and from Proposition 2, it follows that $(r_1, r_2, \dots, r_n) \in \mathbb{B}^n$. Now, it follows from Propositions 1 and 2 that if $(r_1, r_2, \dots, r_n) \in \mathbb{B}^n$, then $p_k(r_1, r_2, \dots, r_n) = f_k(r_1, r_2, \dots, r_n) = 0, \forall k \in \{1, 2, \dots, m\}$, or in other words $(r_1, r_2, \dots, r_n)$ is a solution of system (1). We have obtained a contradiction, which had to be proved.

(ii.b) Let system (2) have no solution. Let us prove that in this case that system (1) also has no solution. From contradiction, let $(b_1, b_2, \dots, b_n) \in \mathbb{B}^n$ be the solution of the system (1). Then, it is obvious that $(b_1^{a_1}, b_2^{a_2}, \dots, b_n^{a_n}) \in \mathbb{B}^n, \forall (a_1, a_2, \dots, a_n) \in \mathbb{B}^n \Rightarrow and_d(b_1^{a_1}, b_2^{a_2}, \dots, b_n^{a_n}) \in \mathbb{B}^1$. Now, it follows from Proposition 1 and Proposition 2 that $f_k(b_1, b_2, \dots, b_n) = p_k(b_1, b_2, \dots, b_n) = 0, \forall k \in \{1, 2, \dots, m\}$, or in other words, $(b_1, b_2, \dots, b_n)$ is the solution of system (2). We have obtained a contradiction, which had to be proved. $\square$

Remark 1. After entering the value of $and_d(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n})$ into system (2) and reducing to a common denominator, each function $f_k(x_1, x_2, \dots, x_n)$ will look as follows:

$$f_k(x_1, x_2, \dots, x_n) = \frac{q_k(x_1, x_2, \dots, x_n)}{h_k(x_1, x_2, \dots, x_n)},$$

where $q_k(x_1, x_2, \dots, x_n), h_k(x_1, x_2, \dots, x_n)$ are polynomials of variables $x_1, x_2, \dots, x_n$, and $h_k(x_1, x_2, \dots, x_n) \neq 0, \forall (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$. Then, it is clear that in the $\mathbb{R}^n$ system, (2) is equivalent to the following system of polynomial equations.

$$\begin{cases} q_1(x_1, x_2, \dots, x_n) = 0 \\ q_2(x_1, x_2, \dots, x_n) = 0 \\ \dots \dots \dots \dots \dots \dots \\ q_m(x_1, x_2, \dots, x_n) = 0 \end{cases}. \quad (3)$$

5. Conclusions

In this paper, firstly, we invented and proved in detail two not-difficult inequalities. Thanks to the proofs of the transformations of these “aesthetic” inequalities into equalities, we have determined (found) suitable smooth (infinitely differentiable) extensions of the discrete logical functions $xor(x_1, x_2, \dots, x_n)$ and $and(x_1, x_2, \dots, x_n)$ to the entire domain $\mathbb{R}^n$. These suitable extensions are applied to systems of logical equations. The system of m logical equations in a constructive way without adding any equations (not field equations and no others) is transformed in $\mathbb{R}^n$ first into an equivalent system of m smooth rational equations so that the solution of the system of m smooth rational equations can be reduced to the problem minimization of the objective function and any numerical optimization methods can be applied since the objective function will be infinitely differentiable. Secondly, again, we transformed the system of m smooth rational equations into an equivalent system of m polynomial equations. This means that any symbolic methods for solving polynomial systems can be used to solve and analyze an equivalent system of m polynomial equations. The equivalence of these systems has been proved in detail.

Thanks to the proofs of these suitable inequalities, we can also conclude that another advantage of the proposed method for transforming the system is that it can be applied to any system described with arithmetic operations and logical operations xor and and .

Author Contributions: Conceptualization, D.N.B.; methodology, D.N.B.; validation, T.E.; formal analysis, D.N.B. and R.N.B.; investigation, K.E.; writing—original draft preparation, R.N.B.; visualization, D.M.; supervision, V.F.; project administration, V.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful to the anonymous reviewers for their valuable comments and suggestions, which helped them to improve the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Brown, F.M. *Boolean Reasoning: The Logic of Boolean Equations*; Kluwer Academic Publishers: Boston, MA, USA, 1990.
2. Hammer, P.L.; Rudeanu, S. *Boolean Methods in Operations Research and Related Areas*; Springer: Berlin, Germany, 1968.
3. Bard, G.V. *Algorithms for Solving Linear and Polynomial Systems of Equations over Finite Fields, with Applications to Cryptanalysis*; University of Maryland: College Park, MD, USA, 2007.
4. Faugere, J.C.; Joux, A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 44–60.
5. Armknecht, F. Improving Fast Algebraic Attacks. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 65–82.
6. Bardet, M.; Faugèrebcd, J.-C.; Salvy, B.; Spaenlehauer, P.-J. On the complexity of solving quadratic boolean systems. *J. Complex.* **2013**, *29*, 53–75. [[CrossRef](#)]
7. Courtois, N. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In *Lecture Notes in Computer Science, CRYPTO 2003*; Boneh, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2729, pp. 176–194.
8. Faugere, J.C. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra* **1999**, *139*, 61–88. [[CrossRef](#)]
9. Faugere, J.C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, Lille, France, 7–10 July 2002; pp. 75–83.
10. Liu, M.; Lin, D.; Pei, D. Fast algebraic attacks and decomposition of symmetric Boolean functions. *IEEE Trans. Inf. Theory* **2011**, *57*, 4817–4821. [[CrossRef](#)]
11. Abdel-Gawad, A.H.; Atiya, A.F.; Darwish, N.M. Solution of systems of Boolean equations via the integer domain. *Inform. Sci.* **2010**, *180*, 288–300. [[CrossRef](#)]
12. Gu, J. How to Solve Very Large-Scale Satisfiability (VLSS) Problems. In *Technical Report UCECETR-90-002*; University of Calgary: Calgary, AB, Canada, 1990.
13. Gu, J. On optimizing a search problem. In *Artificial Intelligence Methods and Applications*; Bourbakis, N.G., Ed.; World Scientific Publishers: Singapore, 1992.
14. Gu, J. Global optimization for satisfiability (SAT) problem. *IEEE Trans. Knowl. Data Eng.* **1994**, *6*, 361–381. [[CrossRef](#)]
15. Gu, J.; Gu, Q.; Du, D. On optimizing the satisfiability (SAT) problem. *J. Comput. Sci. Technol.* **1999**, *14*, 1–17. [[CrossRef](#)]
16. Barotov, D.N.; Muzafarov, D.Z.; Barotov, R.N. On one method for solving systems of Boolean algebraic equations. *Mod. Math. Concept Innov. Math. Educ.* **2021**, *8*, 17–23.
17. Barotov, D.; Osipov, A.; Korchagin, S.; Pleshakova, E.; Muzafarov, D.; Barotov, R.; Serdechnyy, D. Transformation Method for Solving System of Boolean Algebraic Equations. *Mathematics* **2021**, *9*, 3299. [[CrossRef](#)]
18. Barotov, D.N.; Barotov, R.N. Polylinear Transformation Method for Solving Systems of Logical Equations. *Mathematics* **2022**, *10*, 918. [[CrossRef](#)]