Number of Orbits of Group Acting on the Sets of Solutions of Polynomial Equations

Ashot, Minasyan
Yerevan State University
Yerevan, Armenia
e-mail: ashot.minasya@gmail.com

ABSTRACT
Shannon in [1] and Povarov in [2] introduced the notion of types of Boolean functions relating to Boolean functions synthesis by switching circuits. Two Boolean functions over n variables are considered equivalent if one of them can be transformed into another one by an isometric transformation of the vertices of the n-dimensional unit cube. Isometric transformations form a group generated by permutations of the variables and negations of some of the variables.

It is easy to verify that equivalent Boolean functions have an equal complexity for their synthesis by Disjunctive Normal Forms (DNF) and by switching circuits. Tabulating of Shannon-Povarov classes reduces the problem of optimal synthesis of a given Boolean function in the class of DNF or switching circuits to finding an equivalent representative in the table.

In [3-7] the theory of Disjunctive Forms was introduced as a natural generalization of the DNF theory for Boolean functions. The main problem can be defined as follows. Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial over $\mathbb{F}_p^n$, where $\mathbb{F}_p$ stands for a finite field with p elements (p is prime). One has to construct the minimal number of systems of linear equations over n variables, such that the union of the solution sets of the systems coincides with the set of all solutions of the equation $f(x_1, x_2, \ldots, x_n) = 0$. In other words, the problem is to find a cover of the set of the solutions of the polynomial equation with a set of cosets of linear subspaces, using the minimum possible number of cosets. For this problem an analogue of Shannon-Povarov equivalence is the equivalence of polynomials under the action of the group of affine transformations of $\mathbb{F}_p^n$, which transforms cosets into cosets of the same dimension. In this paper we prove the asymptotic formula for the number of equivalence classes of polynomials under the action of the affine group of transformations.

Keywords
Finite field, polynomial function, equivalence classes

1. INTRODUCTION
Let $x = (x_1, \ldots, x_n)$, $f(x)$ and $g(x)$ be polynomials of n variables over finite field $\mathbb{F}_p$. $L_f \subseteq \mathbb{F}_p^n$ is the set of solutions for equation $f(x_1, \ldots, x_n) = 0$. We call f and g equivalent if there are invertible matrix A and vector b so that L_f can be mapped one to one to L_g. For every $x \in L_f, xA + b \in L_g$.

The group of affine transformations of the form $xA + b$ acts on the subsets of F_p^n. We are interested to estimate the number of equivalence classes.

The number of subsets of $\mathbb{F}_p^n$ is 2^{p^n}.

There are $(p^n-1)(p^n-p)(p^n-p^2)\ldots(p^n-p^{n-1})$ invertible matrices and p^n vectors. So the size of the group G_n would be $A_n = (p^n-1)(p^n-p)(p^n-p^2)\ldots(p^n-p^{n-1})p^n$. If we take p^n from all brackets we get

$$A_n = p^{n^2+n}(1-\tfrac{1}{p^n})(1-\tfrac{1}{p^{n-1}})\ldots(1-\tfrac{1}{p}) \approx p^{n^2+n}$$

Let M_n be the number of orbits.

2. LOWER BOUND
In each orbit there could be at most A_n subsets. So

$$M_n \geq \frac{2^{p^n}}{A_n}$$

3. UPPER BOUND
By Bernside's lemma M_n can be calculated using this formula:

$$M_n = \frac{1}{\mid G_n \mid} \sum_{g \in G_n} \psi(g)$$

Here $\psi(g)$ is the number of subsets which are not changed when g acts on it.

$\psi(e)$ would be 2^{p^n}. The next element of G_n that keeps the most of subsets unchanged is the matrix that swaps two coordinates of vectors. Let's denote that matrix by σ. Now we are going to calculate the number of subsets that σ leaves unchanged.

When $i \neq j$ we call the pair of vector $(\alpha_1, \ldots, \alpha_{n-2}, i, j)$ the vector $(\alpha_1, \ldots, \alpha_{n-2}, j, i)$.

In order to get a subset that is invariant to σ we should take the following vectors:

1) Vectors the last two coordinates of which are the same.

2) From the set of vectors the last two coordinates of which are different we should take a pair of vectors at once.

Number of vectors the last two coordinates of which are

the same, is p^{n-1}. So the number of subsets from 1) set is $2^{p^{n-1}}$.

Number of vectors in the remaining set is $p^n - p^{n-1}$. Since we take pairs there are $2^{(p^n-p^{n-1})/2}$ subsets from 2) set.

There are $\binom{n}{2}$ group elements that change a single coordinate so the number of subsets that are invariant to them is $\binom{n}{2}2^{p^{n-1}} \cdot 2^{(p^n-p^{n-1})/2} = \binom{n}{2}2^{(p^n+p^{n-1})/2}$.

The next element of the group that keeps many elements unchanged is the single vector addition.

Let's fix a vector α. In order to get subsets that are invarinat when α acts on them we should again take vectors by pairs. The pair of vector u this time will be $u+\alpha$. Thus, we get $2^{p^n/2}$ subsets that are invariant to α and $p^n 2^{p^n/2}$ subsets that are invarinat to a single vector addition.

If we substitute the numbers we got in the formula of Bernside's lemma we get:

$$M_n = \frac{1}{A_n}\left(2^{p^n} + \binom{n}{2}2^{(p^n+p^{n-1})/2} + p^n 2^{p^n/2} + B_n\right).$$

Where B_n is the sum of functions that are unchanged when other elements are applied.

One can show that:

$$A_n\binom{n}{2}2^{(p^n+p^{n-1})/2} = o(2^{p^n})$$

$$A_n p^n 2^{p^n/2} = o(2^{p^n})$$

$$A_n B_n = o(2^{p^n})$$

Thus, for all $\varepsilon > 0$ and sufficiently large n (depending on ε), we have

$$M_n < \frac{2^{p^n}}{A_n}(1+\varepsilon)$$

So, upper and lower bounds are asimptotically the same.

Theorem 1. *Asymptotic number of equivalence classes of subsets of $\mathbb{F}_p^n$ under the action of the affine group of transformations is equal to*

$$M_n \approx \frac{2^{p^n}}{A_n}$$

It follows from the above that almost all cosets have a maximal size A_n.

REFERENCES

[1] Shannon C. The synthesis of two-terminal switching circuits. BSTJ, 28v. No. 1, 1949, 59—98.

[2] Поваров Г. Н., Математическая теория синтеза контактных (1, k)-полюсников. ДАН СССР, 100, № 5, 1955, 909—912.

[3] Алексанян А., Дизъюнктивные нормальные формы над линейными функциями, Теория и приложения (монография), Издательство Ереванского государственного университета, 1990.

[4] Алексанян А., Реализация булевых функций дизъюнкциями произведений линейных форм, Доклады АН СССР, т. 304, No 4, 1989, стр. 781 – 784.

[5] Алексанян А., Серобян Р., Покрытия, связанные с квадратичными над конечным полем уравнениями, Доклады АН Арм.ССР, т. 93, No 1, 1992, стр. 6 – 10.

[6] В.Габриелян, О метрических характеристиках, связанных с покрытиями подмножеств конечных полей смежными классами линейных подпространств, препринт 04-0603 ИПИА НАН Армении, 2004.

[7] H.K. Nurijanyan, On the Length of the Shortest Linearised Covering for "Almost All" Subsets in a Finite Field, Reports of National Academy of Sciences of Armenia, vol. 110, no.1, pp. 30-34, 2010