Properties of Multiple-Valued Partition Functions

Jon T. Butler[*] Tsutomu Sasao[†] Shinobu Nagayama[‡]

[*]Dept. of Electr. and Comp. Eng., Naval Postgraduate School, Monterey, CA 93943–5121 USA, jon_butler@msn.com
[†]Dept. of Comp. Science, Meiji University, Kawasaki, 214-8571 JAPAN, sasao@ieee.org
[‡]Dept. of Comp. and Network Eng., Hiroshima City University, Hiroshima, 731-3194 JAPAN, s_naga@hiroshima-cu.ac.jp

***Abstract*—We focus on a set of r-valued n-variable functions that are defined by a partition P on the set of r^n input vectors. Specifically, each block of P specifies input vectors, all of which map to the same function value. For example, a symmetric function is defined by a partition where input vectors in the same block are permutations of each other. Given the partition P and the set S of functions associated with P, we analyze the set S' of functions that are a maximal distance from S. Such functions hold promise for use in crypto-systems.**

In this paper, we characterize functions in S'. From this, we compute the distance to their corresponding partition functions. We show that, when r and n increase without bound, this distance approaches the maximum possible, r^n. Bent functions achieve only half the maximum possible distance when n is large. We show that functions a maximal distance from partition functions tend to have a uniform distribution across the r possible function values. Such functions tend to be immune to statistics-based attacks. Finally, we show that, if the set S' of functions is maximally distant from a set S of partition functions, then the converse is true; that is, S is maximally distant from S'.

***Index Terms*—Partition functions, partition set, maximally distant functions, maximally asymmetric functions, bent functions, mutually maximally distant functions, set partitions, characterization and count.**

I. Introduction

The **distance** d between two r-valued n-variable functions, $f(x)$ and $g(x)$, is the number of input vectors for which $f \neq g$. If $f(x) = g(x)$, the distance is 0, and, if all function values differ, then the distance is r^n. The distance d between a function f and a set S of functions is the *minimum* of the distances between f and all the functions $g \in S$. S' is a **maximal distance** from S if it contains all functions whose distance to S is maximum. The distance between two functions has been used in the analysis of crypto-functions, where an attack is successful when the attacker has found a function that is a distance 0 from a function used in the crypto-system. For example, in a crypto-system designed to fend the use of affine functions in an attack, the well-studied bent functions are used, because they are a maximum distance from the set of affine functions. However, binary bent functions are not balanced and are therefore subject to statistics-based attacks. The maximum distance between affine and bent functions is approximately one-half the maximum possible, 2^n. That is, for large n, affine and bent functions are approximately a distance $\frac{2^n}{2}$ apart. In this paper, we show that the maximum distance between multiple-valued partition functions and functions maximally distant from partition functions approaches the maximum, r^n, as n and r grow without bound. That is, the maximum occurs when two functions are different for *every* input vector.

An important subset of partition functions are symmetric functions. The set of functions a maximum distance from symmetric functions, called maximally asymmetric functions, have a binomial distribution similar to random functions [6], [10]. Therefore, one can take a random function, change typically few function values, and create a function that is maximally asymmetric. This is interesting because both symmetric functions and random functions are common in benchmark applications for the evaluation of circuits and algorithms. Maximally asymmetric functions are similar to pseudo random functions [1], [4]. Such functions are essential to crypto-systems and have found application in message authentication systems, distribution of unforgeable ID numbers, dynamic hashing, and friend-or-foe identification [5].

Similarly, bent functions substitute for random sequences. They are useful in the creation of additional channels in synchronous code-division multiple-access (CDMA) systems that employ Walsh sequences for spreading information signals and separating channels [12].

This paper deals with **partition functions**, where a partition of the input vectors exists, such that the function values within each block of the partition are all the same. Partition functions include symmetric functions (unchanged by a permutation of variables), rotation symmetric functions (unchanged by a rotation of input vectors), and degenerate functions (independent of one or more variable). In the case of binary functions, partition functions include linear structure functions ($f(x) = f(x \oplus a)$, where a is fixed) and self-anti-dual functions ($f(x) = f(\overline{x})$). This paper extends [10] so that it applies to multiple-valued functions. It also extends [2], [3], [6], which count maximally asymmetric functions.

II. Definitions

Definition 1. *An r-valued n-variable function f is a mapping from the n dimensional vector space $\mathbf{F}_r^n = \{0, 1, \ldots r-1\}^n$ into the r-element field $\mathbf{F}_r$. One instance of the vector space is an* **assignment of values to the variables** *or* **input vector**.

Definition 2. *A function f is a* **distance** *$d(f, S)$ from a given set S of functions, if the minimum Hamming distance between f and all functions in S is $d(f, S)$. Given a set S of functions, the set S' of functions is said to have a* **maximum distance** *d_S from S if it has the property that, for all $f \in S'$, $d(f, S)$ is maximum; i.e., $d_S = \max_{f \in \mathbf{F}_r^n} \min_{g \in S} d(f, g)$.*

978-1-7281-5406-0/20/$31.00 ©2020 IEEE
DOI 10.1109/ISMVL49045.2020.00-25

IEEE computer society

Example 1. *$d(f, S) = 0$ iff $f \in S$. In the case of two multiple-valued functions, f_1 and f_2, each input vector contributes either 0 or 1 to the Hamming distance. The contribution is 0, if $f_1(A) = f_2(A)$, and is 1 if $f_1(A) \neq f_2(A)$. For example, if the two functions are such that, for all r^n input vectors, the function values disagree, the Hamming distance between the two functions is r^n. The Hamming distance between two identical functions is 0.* ∎

Intuitively, if $f \in S'$, we expect f to have a distance that is "far" from functions in S. It is tempting to believe that if S is a maximum distance from S', then S' is a maximum distance from S.

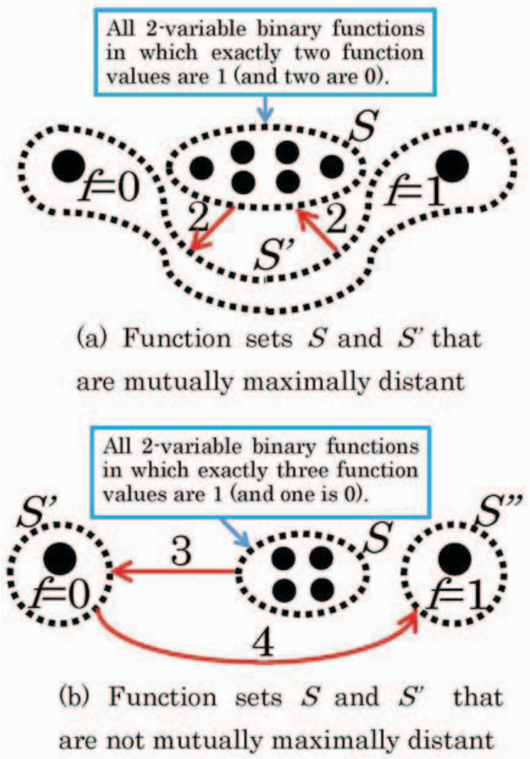
Definition 3. *Two sets of functions, S and S', are* **mutually maximally distant**[1] *if S' is a maximum distance from S and S is a maximum distance from S'.*

Example 2. *Fig. 1(a) shows two sets of functions, S and S', that are mutually maximally distant. Here, S is the set of all 2-variable binary functions in which exactly two function values are 1. The two constant functions, $f(x) = 0$ and $f(x) = 1$, compose a set S' that is a maximum distance from S, where the maximum distance is 2. The red arrow from S to S' labeled "2" shows this. Conversely, the function set S consists of functions that are maximally distant from S'. This is indicated by the other red arrow labeled "2". It follows that the two sets, 1) {f(x) = 1 if exactly two function values are 1} and 2) $\{f(x) = 0, f(x) = 1\}$, are mutually maximally distant.*

Fig. 1(b) shows two sets that are not mutually maximally distant. Here, S is a set consisting of all 2-variable functions in which exactly three function values are 1. The single constant function $f(x) = 0$ compose a set S' that is a maximum distance from S, where the maximum distance is 3. The red arrow from S to S' labelled "3" shows this. On the other hand, the set of functions a maximum distance from $S' = \{f(x) = 0\}$ is $S'' = \{f(x) = 1\}$. The red arrow labeled "4" shows this. It follows that, while $S' = \{f(x) = 0\}$ is maximally distant from S, S is not maximally distant from $S' = \{f(x) = 0\}$. That is, S and S' are not mutually maximally distant. ∎

Tokareva [11] showed that bent functions are mutually maximally distant from the affine functions. In this paper, we show that a set of multiple-valued partition functions is mutually maximally distant from some other set of multiple-valued functions.

Definition 4. *Let P be a set partition of the r^n input vectors into blocks $\{B_1, B_2, \ldots, B_{|P|}\}$, where $|P|$ is the number of blocks in partition P. A* **partition function** *has the property that, for two assignments, A and A' in the same block of set partition P, $f(A) = f(A')$. A* **partition set** *is the set of all partition functions associated with a partition P.*


All 2-variable binary functions in which exactly two function values are 1 (and two are 0).
S
f=0
2
2
S'
f=1
All 2-variable binary functions in which exactly three function values are 1 (and one is 0).
S'
3
S
S''
f=0
f=1
4

(a) Function sets S and S' that are mutually maximally distant

(b) Function sets S and S' that are not mutually maximally distant

Fig. 1: Defining Mutually Maximally Distant Sets

Example 3. *Table I shows the input vectors associated with partition P, which represents the symmetric functions. Since the functions are 2-variable binary, there are four input vectors, 00, 01, 10, and 11. Here, $P = \{\ \{00\}, \{01, 10\}, \{11\}\ \}$, i.e., there are two blocks of one input vector each, and one block with two input vectors. Two input vectors are in the same block of the partition if their corresponding rows are identical. This is a partition set. Table II shows the input vectors associated with partition P which represents the self-anti-dual functions. Here, $P = \{\ \{00, 11\}, \{01, 10\}\ \}$, i.e., there are two blocks of two input vectors each. This is a partition set. Table III shows the set of input vectors which represents the set of affine functions. This is* **not** *a partition set*[2]*.* ∎

III. Characterization of Maximally Distant Multiple-Valued Partition Functions

In the case of bent functions, there is no known characterization. Specifically, there is no known specification that allows the direct enumeration of all bent functions. The only known way to generate all bent functions is to enumerate a set of functions known to contain all bent functions and to test

[1] Tokareva [11], Ivchenko, Medvedev, and Mironova [6], and Oblaukhov [7] refer to "mutually maximally distant function sets" as "metrically regular sets" or "metric complements".

[2] Since all four rows in Table III are different, the partition is trivial. Specifically, each input vector is in a block that is not shared with any other input vector. Table III does not represent a partition set because certain input vectors are missing (8 out of 16 are missing).

TABLE I: Symmetric Functions on Two Binary Variables - A Partition Set, Where $P = \{\ \{00\}, \{01, 10\}, \{11\}\ \}$.

x_1x_2	0	1	x_1x_2	$\overline{x_1x_2}$	$x_1 \vee x_2$	$\overline{x_1 \vee x_2}$	$x_1 \oplus x_2$	$\overline{x_1 \oplus x_2}$
0 0	0	1	0	1	0	1	0	1
0 1	0	1	0	1	1	0	1	0
1 0	0	1	0	1	1	0	1	0
1 1	0	1	1	0	1	0	0	1

TABLE II: Self-anti-dual Functions on Two Binary Variables - A Partition Set, Where $P = \{\ \{00, 11\}, \{01, 10\}\ \}$.

x_1x_2	0	1	$x_1 \oplus x_2$	$\overline{x_1 \oplus x_2}$
0 0	0	1	0	1
0 1	0	1	1	0
1 0	0	1	1	0
1 1	0	1	0	1

TABLE III: Affine Functions on Two Binary Variables - Not a Partition Set.

x_1x_2	0	1	x_1	$\overline{x_1}$	x_2	$\overline{x_2}$	$x_1 \oplus x_2$	$\overline{x_1 \oplus x_2}$
0 0	0	1	0	1	0	1	0	1
0 1	0	1	0	1	1	0	1	0
1 0	0	1	1	0	0	1	1	0
1 1	0	1	1	0	1	0	0	1

each for bentness. For example, all functions whose weight is bent (the number of input vectors for which the function is 1 is $2^{n-1} \pm 2^{n/2-1}$) can be enumerated and each tested for bentness (determine if the Hamming distance to all affine functions is $2^{n-1} \pm 2^{n/2-1}$).

However, it is different for partition functions. The maximally distant functions can be identified by a process that examines the input vectors one block at a time. This process depends on the fact that the maximal distance is the sum of the distances contributed by each block and the distances are determined only by each block independent of the contributions of any other block. Formally,

Definition 5. *Let there be β_i input vectors associated with block B_i of a partition P associated with a set of partition functions. A distribution of β_i input vectors to the r logic values is* **uniform** *if 1) no logic value is assigned more than $\lceil \frac{a_i}{r} \rceil$ input vectors, and 2) no logic value is assigned fewer than $\lfloor \frac{a_i}{r} \rfloor$ input vectors.*

Example 4. *A uniform distribution of input vectors is a distribution that is as even as possible. For example, if $\beta_i = 6$, and $r = 3$, in a uniform assignment, each logic value has two input vectors. If $\beta_i = 7$ and $r = 3$, then, in a uniform distribution, one logic value has three input vectors and the other two have two. On the other hand, if $\beta_i = 6$, and if one logic value has three input vectors, one has two, and one has one, this is not a uniform distribution.* ■

Theorem 1. *An r-valued n-variable function $f(x)$ is maximally distant from a multiple-valued partition set if and only if, for all blocks in the partition, $f(x)$ has a uniform distribution of input vectors to the r logic values.*

Proof:
(only if) Assume that $f(x)$ is maximally distant from a partition function. The distance can be computed as the sum of the distances associated with each block of the partition. Since each block contributes to the maximal distance independently, it must be that all blocks of the partition contribute the maximum distance. On the contrary, assume that at least one block does not have a uniform distribution of input vectors to the r logic values. It follows that there is a logic value v in a block β_i that occurs more often than $\lceil \frac{\beta}{r} \rceil$, or there is a logic value v in a block β_i that occurs less often than than $\lfloor \frac{\beta_i}{r} \rfloor$. It follows that the (partial) distance to a partition function whose block β_i maps to v is less than the maximum possible. It follows that the total distance is less than maximum. This is a contradiction.
(if) Assume that $f(x)$ has a uniform distribution of values to variables to the r logic values in all blocks of the partition. On the contrary, assume the $f(x)$ is not maximally distant from a set of partition functions. If follows that at least one block β_i fails to achieve the maximum distance to partition function. However, the maximum distance for β_i is achieved only when the logic values within β_i are uniformly distributed. It follows that $f(x)$ has a distribution of logic values within β_i that is not uniformly distributed. This is, a contradiction. □

Theorem 1 is a complete characterization of functions that are maximally distant from a set of partition functions.

IV. Maximal distances from multiple-valued partition functions

Given a partition set S of functions associated with a partition P, we determine, in this section, the distance D_P to the maximally distant set S'. We know that this distance is the sum of distance contributions from each block in the partition. Further, the contribution from each block is independent of the contribution from other blocks.

Theorem 2. *The distance D_P between the set S of r-valued n-variable partition functions associated with partition P, and its maximally distant set S' is*

$$D_P = r^n - \sum_{i=1}^{|P|} \left\lceil \frac{\beta_i}{r} \right\rceil, \qquad (1)$$

where $|P|$ is the number of blocks in partition P.

Proof: The sum in (1) enumerates the blocks in partition P. Each block contributes β_i input vectors to the total distance, except for matches across a uniform distribution. This latter contribution is $\lceil \frac{\beta_i}{r} \rceil$, since the logic value(s) with the most matches contributes the least partial distance. Thus, D_P is $\sum_{i=1}^{|P|} (\beta_i - \lceil \frac{\beta_i}{r} \rceil)$. Substituting $r^n = \sum_{i=1}^{|P|} \beta_i$, yields (1). □

Let $\beta_i = kr$, for some integer $k \geq 1$. Then, $\lceil \frac{\beta_i}{r} \rceil = k$, and, for $n \to \infty$, $|P| \to \frac{r^n}{kr} = \frac{r^{n-1}}{k}$. Thus, $D_P \to r^n - \sum_{i=1}^{|P|} k = r^n - \frac{r^{n-1}}{k} k = (1 - \frac{1}{r}) r^n$. Therefore,

Corollary 1. *When $\beta_i = kr$ for some integer $k \geq 1$, $n \to \infty$, and $r \to \infty$, the distance D_P between a set of r-valued n-variable partition functions associated with partition P, and its maximally distant set approaches r^n, the maximum possible distance between any two r-valued n-variable functions.*

Note that, when $r = 2$, this distance spans approximately one-half only of the maximum possible distance. We observed earlier that, in the case of binary bent functions, the distance between affine functions and (the maximally distant) bent functions is $\frac{2^n}{2}$, which is one-half of 2^n, the maximum possible distance between two n-variable binary functions.

V. Count of the maximally distant functions from multiple-valued partition functions

Given the characterization of functions that are maximally distant from a multiple-valued partition function, shown in Section III, we can now calculate the number of functions in that set. Specifically, we can calculate the number of ways a uniform distribution can exist in each block. As a result, the number of maximally distant functions will be expressed as a product, where each component of the product corresponds to the number of ways input vectors can be chosen so that the maximum distance is achieved within the block.

Theorem 3. *The number of functions that are maximally distant from the set of partition functions associated with partition P is given as*

$$N_P = \prod_{i=1}^{|P|} \binom{r}{\phi_i} \frac{\beta_i!}{\lfloor \frac{\beta_i}{r} \rfloor !^{r-\phi_i} (\lfloor \frac{\beta_i}{r} \rfloor + 1)!^{\phi_i}}, \tag{2}$$

where $|P|$ is the number of blocks in partition P, $\beta_i = |B_i|$ is the number of input vectors in block B_i, and where

$$\phi_i = \beta_i - r \left\lfloor \frac{\beta_i}{r} \right\rfloor \tag{3}$$

is the number of logic values that is 1 more than the number containing the minimum number of input vectors.

Proof: We calculate the number of functions that are a maximum distance from a partition set of functions by multiplying the number of ways in each block to achieve a uniform distribution of input vectors to the r function logic values. Thus, N_P in (2) is expressed as a product over the $|P|$ blocks of P. By definition, over all the input vectors within each block, the partition function values are the same. Thus, functions that are maximally distant are distributed uniformly. In counting the maximally uniform distributions, we can think of the logic values as bins and the input vectors as balls. We seek to count the distributions of distinct balls into distinct bins where each bin has the same or nearly the same number of balls. If the number of input vectors β_i to the ith block is a multiple of r, each logic value will occur exactly $\lfloor \frac{\beta_i}{r} \rfloor$ times, which is the perfectly uniform distribution. If β_i is a multiple of r plus 1, in the uniform distribution, all logic values have $\lfloor \frac{\beta}{r} \rfloor$ input vectors except one, which will have 1 more. Which logic value has 1 more can be specified in $r = \binom{r}{1}$ ways. In general, there will be $\phi_i = \beta_i - r \lfloor \frac{\beta_i}{r} \rfloor$ logic values in (2) with 1 more input vector. Which of the r logic values have 1 more is specified in (2) in $\binom{r}{\phi_i}$ ways. We count each distribution as permutation of the distinct input vectors of values to the variables ($\beta_i!$), except any permutation within a bin corresponding to a logic value does not change the sought after distribution. That is, a rearrangement of input vectors within each 'logic value' bin leaves unchanged the distribution. Thus, for each combination $\binom{r}{\phi_i}$, there are $(\lfloor \frac{\beta_i}{r} \rfloor !^{r-\phi_i} (\lfloor \frac{\beta_i}{r} \rfloor + 1)!^{\phi_i})$ possible rearrangements, for a total of $\binom{r}{\phi_i} \lfloor \frac{\beta_i}{r} \rfloor !^{r-\phi_i} (\lfloor \frac{\beta_i}{r} \rfloor + 1)!^{\phi_i})$ arrangements of input vectors for each block. □

VI. Properties of maximally distant functions

A. Functions related by a permutation of variables

Theorem 4. *Let S be a function set with the property that if $f \in S$, then $f' \in S$, where f' is f with function values permuted by some permutation. Then, the maximally distant set S' to S has the property that if $g \in S'$, then $g' \in S'$, where g' is g with function values permuted by the same permutation.*

Proof: Let S be a function set with the property that if $f \in S$, then $f' \in S$, where f' is f with function values permuted by some permutation. We showed in Theorem 1 that, given a set of functions S, the set of all maximally distant functions is derived as a uniform distribution of logic values across each block. Further, this is a complete characterization of the maximally distant functions. A permutation of the logic values across the construction of S' leaves the distances between functions unchanged, but assures that, if function $g \in S'$, then $g' \in S'$, where g' is g with function logic values permuted by the same permutation. □

The property that a set S of functions contains all functions derived from other functions in S by permuting function values is a common one. It occurs in symmetric functions and bent functions, for example.

B. Distribution of functions that are maximally distant from partition functions

We note that functions maximally distant from partition functions tend to have a uniform distribution of function values. That is, in constructing such functions, we use uniform distributions of logic values across the partition blocks. Since this occurs for all blocks in the partition, this tends to make the overall distribution uniform. We have

Theorem 5. *Let S be a partition set of functions, and S' its maximally distant set. Then, the functions in S' are uniformly distributed with respect to function values.*

In a cryptographic application, functions in S' will have the desirable characteristic of having uniformly distributed function values. Such functions have immunity to statistics-based attacks.

VII. Partition Functions and Their Maximally Distant Functions Are Mutually Maximally Distant

As noted in Section II Definitions, the set of bent functions is mutually maximally distant from the set of affine functions. In this section, we show that a similar statement is true of partition functions and functions maximally distant from partition functions.

Theorem 6. *Let S be a partition set corresponding to a partition P, and let S' be the set of functions that are maximally distant from S. Then, S is also maximally distant from S'.*

Proof: Let $P = \bigcup_{i \in I} B_i$ be the partition of $\mathbf{F}_r^n = \{0, 1, \ldots r-1\}^n$, the set of input vectors. Let $i \in \{1, 2, \ldots k\}$ index the k blocks of P. Let $\beta_i = |B_i|$ be the number of input vectors in block B_i. Let $g \in S'$. Then, $d_S = d(g, S)$. Theorem 1 shows that the distribution of logic values to each block B_i of g is uniform. That is, each logic value occurs no more than $\lceil \frac{\beta_i}{r} \rceil$ times and no less than $\lfloor \frac{\beta_i}{r} \rfloor$ times in every block of B_i of g, and this is a complete characterization of g.

Let f be maximally distant from S'. Then, $d(f, S') \geq d_S$; otherwise, $d_S \neq d(g, S)$. Contrary to the hypothesis, assume that $f \notin S$. It follows that there is at least one ℓ, such that B_ℓ contains at least two different logic values. That is, block B_ℓ does not satisfy the requirement on partition functions that all input vectors in B_ℓ map to the *same* logic value. Since the distribution of logic values to block B_ℓ is not balanced, at least one logic value, ρ, occurs more than $\lceil \frac{k_l}{r} \rceil$ times or less than $\lfloor \frac{k_l}{r} \rfloor$ times. Consider the contribution of B_ℓ to $d(f, S')$. When there is balance, the contribution is $\beta_i - \lfloor \frac{\beta_i}{r} \rfloor$. When there is imbalance, the contribution is strictly less, specifically for input vectors that map to the logic values that are over-represented in the unbalanced distribution. We have $d(f, S') \leq \sum_{i \in \{1,2,\cdots k\}} C_i^{unbal} < \sum_{i \in \{1,2,\cdots k\}} C_i^{bal} = d_S$, which contradicts $d(f, S') \geq d_S$, where C_i^{unbal} is the contribution to the distance by block B_i in the case where at least one block is unbalanced, and C_i^{bal} is the contribution to the distance by block B_i in the case where all blocks are balanced. □

VIII. Concluding Remarks

Partition sets are based on a set partition P of the input vectors. Specifically, partition sets have the property that all input vectors in the same block of P map to the same function value. For example, symmetric functions are partition functions in which all blocks contain input vectors that are permutations of other input vectors in the same block. Other partition functions include rotation symmetric functions, and degenerate functions. In this paper, we characterize the set S' of functions that are maximally distant from a partition set S. From this, we compute the distance between S and S' and the number of functions in S'. The distance is a metric for how effective a function in S' is in a cryptographic application, in which a random-like function is sought for encryption. We show that when $n \to \infty$ and $r \to \infty$, where $\beta_i = kr$, for some integer $k \geq 1$, the maximal distance between S and S' approaches the maximum possible between two functions. Namely, this distance approaches r^n, which occurs between two functions that differ in *all* input vectors.

We also show that functions which are a maximal distance from a set S of functions tend to be balanced. That is, their function values tend to be evenly balanced among the r possible function values. This is a benefit because it reduces the cryptosystem's vulnerability to statistics-based attacks.

Finally, we show that partition functions are mutually maximally distant from another set. That is, if S is a partition set, then the maximally distant set of functions S' has the property that S is maximally distant from S'.

We finish with a conjecture.

Conjecture 1. *Let S be a set of r-valued n-variable functions, and let S' be the set of functions that are maximally distant from S. S and S' are mutually maximally distant if and only if S has the property that, if $f \in S$ then $f' \in S$, where f' is f with the function values permuted.*

In this paper, we show in Theorem 6 that Conjecture 1 is true for the special case where S is a partition set.

Fig. 1 also corroborates Conjecture 1. That is, in Fig. 1a, which shows two mutually maximal functions, all functions in $S(S')$ occur as the complement function of another function in $S(S')$. On the other hand, in Fig. 1b, which shows a set S of functions and a set S' of functions that are maximally distant from S, such that S is *not* maximally distant from S', functions in S do *not* occur as complements.

Also, note that affine functions and bent functions are mutually maximally distant from each other and have the complemented property. It is interesting that, although affine functions are *not* partition functions, they are complement functions.

Finally, the trivial partition P consisting of blocks, all of which contain a single input vector, presents a potentially absurd proposition. From (1), the distance to the maximally distant set is $D_P = 0$, while from (2), the number of functions in the maximally distant set is $N_P = r^{r^n}$. That is, the set of all functions is 'maximally distant' from the partition set consisting of all functions, with the maximum distance being 0. Every function in S' is a distance 0 from one function in S, and, conversely, every function in S is a distance 0 from one function in S'. Thus, S and S' are mutually maximally distant from each other with the distance being 0. When the distance between S and S' is greater than 0, S and S' are necessarily disjoint. When the distance is 0, S and S' are **non**disjoint and each consists of all input vectors.

Acknowledgment

This research is partly supported by a Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research and by the JSPS KAKENHI Grant (C), No.16K00079, 2018. Comments by three referees improved this manuscript.

References

[1] A. Bogdonov and A. Rosen, “Pseudorandom functions: Three decades later,” in Y. Lindell(ed.) *Tutorials on the Foundations of Cryptography*, 2017 Springer International Publishing AG. Part of Springer Nature. pp. 79-158.

[2] J. T. Butler and T. Sasao, “Maximally asymmetric multiple-valued functions”, *49th International Symposium on Multiple-Valued Logic*, May 2019, pp. 188–193.

[3] J. T. Butler and T. Sasao, “Enumerative analysis of asymmetric functions”, *Reed-Muller Workshop*, May 24, 2019, Fredricton, New Brunswick, Canada, 2019.

[4] O. Goldreich, S. Goldwasser, and S. Micali, “How to construct random functions,” *Journal of the Association for Computing Machinary*. Vol. 33, No. 4, October 1986, pp. 792-807.

[5] O. Goldreich, S. Goldwasser, and S. Micali, “On the cryptographic application of random functions,” G. R. Blakley and D. Chaum (Eds.): *Advances in Cryptology - CRYPT0 ’84*, *Lecture Notes in Computer Science* 196, pp. 276-288, 1985.

[6] I. Ivchenko, Y. I. Medvedev, V. A. Mironova, “Symmetric Boolean functions and their metric properties matrices of transitions of differences when using some modular groups” (in Russian), *Mat. Vopr. Kriptogr.* 4:4, pp. 49–63, 2013.

[7] A. K. Oblaukhov, “Metric complements to subspaces in the Boolean cube” (in Russian), *Diskretnyi Analiz i Issledovanie Operatsii*, Vol. 23, No. 3, pp. 93–106, 2016. (Abstract: J. Appl. Ind. Math. 10:3, pp. 397–403, 2016).

[8] T. Sasao, *Switching Theory for Logic Synthesis*, Kluwer Academic Publishers, 1999.

[9] P. Solé, “A quaternary cyclic code and a family of quadraphase sequences with low correlation properties,” *Coding Theory and Applications, Lecture Notes in Computer Science,* New York: Springer-Verlag, 1989, vol. 388, pp. 193–201.

[10] P. Stănică, T. Sasao, and J. T. Butler, “Distance duality on some classes of Boolean functions”, *Journal of Combinatorial Mathematics and Combinatorial Computing*, November 2018, Vol. 107, pp 181–198.

[11] N. Tokareva, “Duality between bent functions and affine functions”, *Discrete Mathematics* 312 (2012), 666–670.

[12] K, Yang, Y-K Kim, and P. V. Kumar, “Quasi-orthogonal sequences for code-division multiple-access systems”, *IEEE Transactions on Information Theory*, May 2000, Vol. 46, pp. 982-993.