Maximally Asymmetric Multiple-Valued Functions

Jon T. Butler
Department of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA 93943–5121 USA
Email: jon_butler@msn.com

Tsutomu Sasao
Department of Computer Science
Meiji University
Kawasaki-shi, Kanagawa-ken, 214-8571 JAPAN
Email: sasao@ieee.org

***Abstract*—The asymmetry of a function $f(x_1, x_2, \ldots, x_n)$ is the fewest elements of the range of f that must be changed so that f becomes a symmetric function. The functions with maximal asymmetry for the case of r-valued n-variable functions have been characterized and counted for $r = 2$ in two previous papers. In this paper, we extend these results to $r > 2$. We do this for two types of symmetry, functions whose value is unchanged by 1) any permutation of the variable labels and by 2) any permutation of variable labels and variable values. We also derive the maximum possible asymmetry. We show that, as $n \to \infty$ and r is fixed, the maximum asymmetry approaches $(r-1)r^{n-1}$.**

***Index Terms*—Asymmetric functions, maximally asymmetric functions, multiple-valued, symmetric functions, v-symmetry, vv-symmetry, partitions of integers, characterization and count**

I. Introduction

The **asymmetry** of a function f is the minimum number of function values that must be changed so that f becomes a symmetric function. All symmetric functions have asymmetry 0. We are interested in the set of functions that are *maximally* asymmetric. Maximally asymmetric functions share an important property with random functions. Namely, the distributions of the function values of maximally asymmetric functions and random functions are similar [4]. One result of this is that we can take a random function, change relatively few function values, and produce a function that is maximally asymmetric. This is interesting because both symmetric functions and random functions are prominent in benchmark applications for the evaluation of circuits and algorithms. Maximally asymmetric functions share properties with pseudo random functions (PRFs) [2], [5]. 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 [6].

Similarly, bent functions serve as a 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 [11]. On the other hand, binary bent functions have a pallid distribution by weight; among all binary bent functions, there are only two weights, $2^{(n-1)} \pm 2^{(\frac{n}{2}-1)}$. Maximally asymmetric functions, on the other hand, have a distribution that is more like random functions, as shown for binary functions in Fig. 1 [10]. Also, bent functions are hard to generate, unlike maximally asymmetric functions.

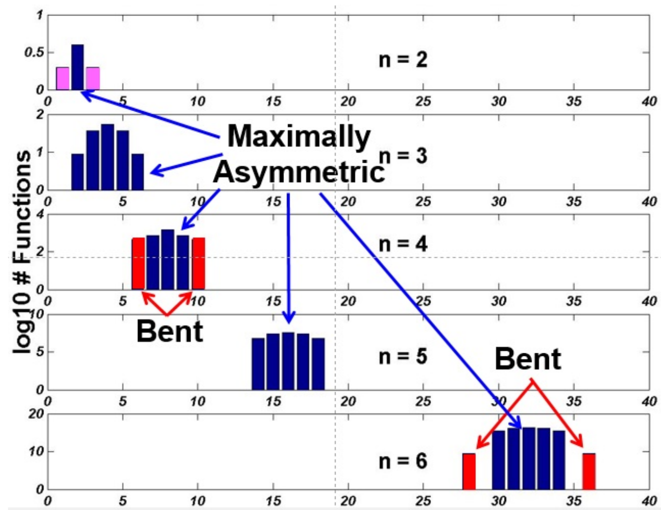

Fig. 1: [10] Distribution of Binary Maximally Asymmetric and Bent Functions By Weight

This paper extends three papers. It extends [3], which counts two kinds of multiple-valued *symmetric* functions; functions that are unchanged by a 1) permutation of variable labels or by a 2) permutation of variable labels and variable values. This paper also extends [7], [10], which count *binary maximally asymmetric* functions. In this paper, we count *multiple-valued maximally asymmetric* functions, and we do it for the two kinds of symmetry. As a further justification for the study of multiple-valued functions, we note that quarternary functions have been used in the analysis of quadrature phase shift keying CDMA-type applications [1], [9], [11].

II. Definitions

An n-variable r-valued 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 $\mathbf{F}_r$.

Definition 1. *A function is* **v-symmetric** *(variable-symmetric) if it is unchanged by any permutation of variable labels. A function is* **vv-symmetric** *(variable/value-symmetric) if it is unchanged by any permutation of the variable labels and any permutation of the variable values [3].*

Example 1. *Table I shows two 3-variable 3-valued functions, f_1 and f_2. Here, f_1 is v-symmetric but not vv-symmetric, while*

f_2 *is vv-symmetric (and also v-symmetric).* ■

TABLE I: Examples of v-Symmetric (f_1) and vv-Symmetric (f_2) Functions

x_1	x_2	x_3	f_1	f_3	f_2	f_4
0	0	0	1	0	0	0
1	1	1	1	2	0	1
2	2	2	2	2	0	2
0	0	1	2	0	1	0
0	1	0	2	1	1	0
1	0	0	2	2	1	0
0	0	2	0	0	1	0
0	2	0	0	1	1	0
2	0	0	0	2	1	0
0	1	1	1	0	1	1
1	0	1	1	1	1	1
1	1	0	1	2	1	1
0	2	2	2	0	1	1
2	0	2	2	1	1	1
2	2	0	2	2	1	1
1	1	2	1	0	1	2
2	1	1	1	1	1	2
1	2	1	1	2	1	2
1	2	2	2	0	1	2
2	1	2	2	1	1	2
2	2	1	2	2	1	2
0	1	2	0	0	2	0
0	2	1	0	0	2	0
1	0	2	0	1	2	1
1	2	0	0	1	2	1
2	0	1	0	2	2	2
2	1	0	0	2	2	2

TABLE II: The alpha vectors of f_1 and f_2 from Table I.

α_0	α_1	α_2	f_1	f_2
3	0	0	1	0
2	1	0	2	1
2	0	1	0	1
1	2	0	1	1
1	1	1	0	2
1	0	2	2	1
0	3	0	1	0
0	2	1	1	1
0	1	2	2	1
0	0	3	2	0

TABLE III: The beta vectors of f_2 from Table I.

β_0	β_1	β_2	f_2
3	0	0	0
2	1	0	1
1	1	1	2

Definition 2. *A v-symmetric function is specified by the function values associated with* **alpha vectors**, $\overrightarrow{\mathcal{A}} = (\alpha_0, \alpha_1, \ldots, \alpha_{r-1})$*, where* α_i *is the number of variables that have logic value* i*, where* $\sum_{i=0}^{r-1} \alpha_i = n$*.*

Example 2. *Shown in Table II are the alpha vectors of functions* f_1 *and* f_2 *from Table I.* ■

Definition 3. *A vv-symmetric function is specified by the function values associated with* **beta vectors** $\overrightarrow{\mathcal{B}} = (\beta_0, \beta_1, \ldots, \beta_{r-1})$*, where* β_0 *is the number of variable values that are the most polific,* β_1 *is the number of variable values that are the next most prolific, etc., and where* $\sum_{i=0}^{r-1} \beta_i = n$*. Here,* $n \geq \beta_0 \geq \beta_1 \geq \ldots \geq \beta_{r-1} \geq 0$*, and if two alpha vectors are permutations of each other, there is exactly one corresponding beta vector, the lexicographically highest alpha vector. Each beta vector represents an integer partition on* n *with* r *or fewer parts.*

Example 3. *Shown in Table III are the beta vectors of function* f_2 *from Table I.* ■

Example 4. *In this case of* $r = 2$*, a v-symmetric function is specified by* $n+1$ *function values, while a vv-symmetric function is specified by* $\lfloor \frac{n+1}{2} \rfloor$ *function values. For* $r = 2$ *and* $n = 2$*, there are eight v-symmetric functions,* $f = 0$*,* $x_1 x_2$*,* $x_1 \oplus x_2$*,* $x_1 \vee x_2$*, and their complements, and there are two vv-symmetric functions,* $f = x_1 \oplus x_2$*, and its complement.* ■

Definition 4. *The* **v-asymmetry** *of a function* f*, denoted by* $v\_asym(f)$*, is the minimum number of truth table entries that must be changed to convert* f *to a v-symmetric function; that is,*

$$v\_asym(f) = d(f, S_v) = \min\{d(f,s) | s \in S_v\},$$

where S_v *is the set of* n*-variable v-symmetric functions and,* d *is the Hamming distance function.*

Definition 5. *Similarly, the* **vv-asymmetry** *of a function* f*, denoted by* $vv\_asym(f)$*, is the minimum number of truth table entries that must be changed to convert* f *to a vv-symmetric function; that is,*

$$vv\_asym(f) = d(f, S_{vv}) = \min\{d(f,s) | s \in S_{vv}\},$$

where S_{vv} *is the set of* n*-variable vv-symmetric functions, and* d *is the Hamming distance function.*

Definition 6. *A* **maximally v-asymmetric function** f *has the maximum v-asymmetry among all* n*-variable functions. A* **maximally vv-asymmetric function** f *has the maximum vv-asymmetry among all* n*-variable functions.*

Example 5. f_3 *is maximally v-symmetric because it has v-asymmetry 16, which, we know is maximum among 3-valued, 3-variable functions.* f_4 *is maximally vv-symmetric because it has vv-asymmetry 18, which, we know is maximum among 3-valued, 3-variable functions.* ■

III. THE NUMBER OF SYMMETRIC FUNCTIONS

Lemma 1. *[3] The number* $N_v(n,r)$ *of* r*-valued* n*-variable v-symmetric functions is*

$$N_v(n,r) = r^{\binom{n+r-1}{r-1}}, \tag{1}$$

where $\binom{n+r-1}{r-1}$ *is the number of ways to choose* r *objects from* n *with repetition.*

From this, we can conclude that the number of function values needed to completely specify a v-symmetric functions is $\binom{n+r-1}{r-1}$, one for each element of the alpha vector.

Lemma 2. *[3] The number* $N_{vv}(n,r)$ *of* r*-valued* n*-variable vv-symmetric functions is*

$$N_{vv}(n,r) = r^{p(n,r;n)}, \tag{2}$$

where $p(\sigma, r; n)$ *is the number of partitions of* n *with* r *or fewer parts and with no part greater than* σ*.*

From this, we can conclude that the number of function values needed to specify completely vv-symmetric functions is $p(n, r; n)$, one for each element of the beta vector.

Example 6. *The third and fourth columns of Table V show the number of r-valued n-variable v-symmetric and vv-symmetric functions, respectively, for $2 \leq n \leq 8$ and $2 \leq r \leq 6$. This occurs in the columns labeled #v-S and #vv-S, respectively. For larger values of n and r, there are many more v-symmetric functions than there are vv-symmetric functions.* ■

IV. Characterization of Maximally v-Asymmetric and Maximally vv-Asymmetric Functions

A. Maximally v-Asymmetric Functions

In determining the v-asymmetry of a given function f, we start by partitioning the vectors according to the assignment of values to the variables. For example, consider function f_1 in Table I. Since f_1 is v-symmetric, f_1 has the same value (2) for $x_1x_2x_3 = 001,\ 010,$ and 100, for example. A critical observation is that these three assignments contribute a value to the maximum v-asymmetry of f_1 that is *independent* of *all* other assignments. The contribution to the v-asymmetry of a maximally v-asymmetric function occurs when the values of the function for $x_1x_2x_3 = 001,\ 010,$ and 100 are uniformly distributed across all three logic values, since this maximizes the minimum distance to a v-symmetric function. In this case, a uniform distribution occurs with one 0, one 1, and one 2, and creates a distance contribution of 2. The following theorem extends the result in [7], [10] to general r-valued functions, where $r > 2$. Here, we characterize maximally v-asymmetric functions.

Theorem 1. *An n-variable r-valued function f is maximally v-symmetric if and only if the logic values of f are uniformly distributed across all assignments of values to variables that correspond to the same alpha vector component.*

An important observation about maximally asymmetric functions is that each alpha vector contributes a part of the total asymmetry in a sum across all alpha vectors. From this and Theorem 1, we can compute the v-asymmetry of *maximally* v-asymmetric functions.

Theorem 2. *Let $\overrightarrow{\mathcal{A}}_i$ be the i-th alpha vector of a function f, and A_i the number of assignments of values to variables corresponding to $\overrightarrow{\mathcal{A}}_i$. Then, a maximally v-asymmetric n-variable r-valued function has v-asymmetry $\Theta_v(n,r)$, where*

$$\Theta_v(n,r) = \sum_{i=1}^{\binom{n+r-1}{r-1}} \left\lfloor A_i \frac{r-1}{r} \right\rfloor. \tag{3}$$

Example 7. *The fifth column of Table V shows, in bold, $\Theta_v(n,r)$, for $2 \leq n \leq 8$ and $2 \leq r \leq 6$.* ■

B. Maximally vv-Asymmetric Functions

Theorem 3. *An n-variable r-valued function f is maximally vv-asymmetric if and only if the logic values of f are uniformly distributed across all assignments of values to variables that correspond to the same beta vector.*

From this, we can compute the vv-asymmetry of *maximally* vv-asymmetric functions.

Theorem 4. *Let $\overrightarrow{\mathcal{B}}_i$ be the i-th beta vector, and B_i the number of assignments of values to variables corresponding to $\overrightarrow{\mathcal{B}}_i$. Then, a maximally vv-asymmetric n-variable r-valued function has vv-asymmetry $\Theta_{vv}(n,r)$, where*

$$\Theta_{vv}(n,r) = \sum_{i=1}^{p(n,r;n)} \left\lfloor B_i \frac{r-1}{r} \right\rfloor, \tag{4}$$

where $p(n,r;n)$ is the number of partitions of n with no more than r parts.

Example 8. *The sixth column of Table V shows, in bold, $\Theta_{vv}(n,r)$, for $2 \leq n \leq 8$ and $2 \leq r \leq 6$.* ■

Along with Θ_v and Θ_{vv}, Table V shows, also in bold, the maximum possible distance between n-variable r-valued functions, as 'Max.', in the seventh column. This is r^n, the size of the truth table, which corresponds to a different function value for *every* assignment of values to the variables. The data shows that, as $n \to \infty$ and r is fixed, $\Theta \to \frac{r-1}{r} r^n$. We can show this analytically, as follows.

Consider the case of $\Theta_v(n,r)$, as given in (3). The case for $\Theta_{vv}(n,r)$ is similar. The sum in (3) enumerates all possible A_i, assignments of values to the variables. Each contributes in proportion as $\lfloor \frac{r-1}{r} \rfloor$. When n is large and r is fixed, the floor function has negligible effect, and the proportion is close to $\frac{r-1}{r}$. This outlines the proof of the following.

Theorem 5. *Let $\Theta_v(n,r)$ and $\Theta_{vv}(n,r)$ be the maximal v-asymmetry and vv-asymmetry, respectively, among n-variable r-valued functions. Then,*

$$\Theta_v(n,r) \to (r-1)r^{n-1} \text{ and } \Theta_{vv}(n,r) \to (r-1)r^{n-1}, \tag{5}$$

as $n \to \infty$ and r is fixed.

It is interesting to compare the maximal asymmetry associated with binary asymmetric functions and the "bent" distance associated with binary bent functions. Substituting $r = 2$ into (5) yields the maximal asymmetry associated with both v-symmetric and vv-symmetric binary functions as 2^{n-1} in the limit as $n \to \infty$. This is the minimum of the distance between v-symmetric and vv-symmetric functions and v-asymmetric and vv-asymmetric functions, respectively. The minimum of the distance between affine functions and bent functions is the "bent" distance $2^{n-1} - 2^{\frac{n}{2}-1}$. This is less, but approaches 2^{n-1}, as $n \to \infty$. That is, for large n, both distances are nearly the same. Indeed, they are both approximately one-half the maximum distance between two functions that are the complement of each other.

V. Count of the Maximally v-Symmetric and Maximally vv-Symmetric Functions

A. v-Asymmetric Functions

Theorem 6. *The number of n-variable r-valued v-asymmetric functions $N_v(n,r)$ is*

$$N_v(n,r) = \prod_{i=1}^{p(n,r;n)} \left[\frac{r!}{(r-R_i)!R_i!} \quad \frac{A_i!}{(Q_i)!^{(r-R_i)}(Q_i+1)!^{R_i}} \right]^{G_i} \tag{6}$$

where

1) n *is the number of variables and* r *is the number of values,*
2) $p(n, r; n)$ *is the number of partitions on* n *with* r *or fewer parts,*
3) G_i *is the number of groups associated with the* i*-th partition. Specifically, if the* i*-th partition is* $n^{m_n} \ldots 2^{m_2} 1^{m_1}$*, where* j^{m_j} *is a part of size* j *and* m_j *is the number of such parts, then*

$$G_i = \binom{r}{m_n}\binom{r - m_n}{m_{n-1}}\binom{r - m_n - m_{n-1}}{m_{n-2}} \ldots \binom{r - m_n - m_{n-1} - \ldots - m_2}{m_1}, \quad (7)$$

4) A_i *is the number of assignments of values to variables in all parts associated with the* i*-th partition. Specifically,*

$$A_i = \frac{n!}{n!^{m_n}(n-1)!^{m_{n-1}} \ldots 1!^{m_1}}, \quad \text{and} \quad (8)$$

5) Q_i *is the quotient and* R_i *is the remainder resulting from the division* $\frac{A_i}{r}$*.*

Proof: Each partition on n with $\rho \leq r$ parts specifies how ρ logic values are assigned to n variables when the corresponding functions are symmetric. So, if the partition is

$$n^{m_n}(n-1)^{m_{n-1}} \ldots 1^{m_1}, \quad (9)$$

then there are m_n sets of n variables and every variable within each set is assigned to a distinct logic value, there are m_{n-1} sets of $n-1$ variables and every variable within each set is assigned to a distinct logic value, ... , and there are m_1 sets of 1 variable[1] and every variable within each set is assigned to a distinct logic value. The partition does not specify which specific logic value is assigned to a specific variable, only that there are so many sets of variables of a certain size that are assigned the same logic value. We note that $m_n + m_{n-1} + \ldots + m_1 = \rho \leq r$ and $n \cdot m_n + (n-1) \cdot m_{n-1} + \ldots + 1 \cdot m_1 = n$.

When specific logic values are assigned, each partition forms groups of assignments to variables such that any permutation of the variable labels preserves the distribution of variable values. The number of groups associated with the i-th partition is given with the understanding that each m_j in (7) is associated with the i-th partition.

We next compute A_i, the number of assignments of values to variables that exist within each group associated with the i-th partition. This is (8). $n!$ counts the arrangements of variables when all are distinct. However, they are not all distinct. There are m_n sets of n variables that have the same value, m_{n-1} sets of $n-1$ variables that have the same value, ... , and m_1 sets of 1 variable that have the same value.

From Theorem 1, a function has maximum v-asymmetry if there is a uniform distribution of function values across the assignments to variables that map to the same function value in a symmetric function. That is, a maximally v-asymmetric function has the property that, for each of the G_i groups, r logic values must be distributed uniformly across the A_i assignments of values that are in all groups. A uniform distribution is specified by the quotient Q_i and remainder R_i of the division A_i/r. That is, $Q_i + 1$ assignments will map to $R_i (< r)$ values each, while Q_i assignments will map to $r - R_i$ values each.

It now remains only to count how a uniform distribution of logic values can occur across the logic values and across the assignments of values to the variables. With respect to the logic values, the distribution occurs as

$$L_i = \frac{r!}{(r - R_i)! R_i!}. \quad (10)$$

With respect to the distribution across assignments of values to variables, the distribution is divided by those function values having $Q_i + 1$ assignments and those having Q_i assignments, and are distributed as

$$V_i = \frac{A_i!}{Q_i!^{r - R_i}(Q_i + 1)!^{R_i}}. \quad (11)$$

Thus, the total number of maximally v-symmetric n-variable r-valued functions is

$$N_v(n, r) = \prod_{i=1}^{p(n,r;n)} [L_i V_i]^{G_i}. \quad (12)$$

Substituting (10) and (11) into (12) completes the proof. □

Example 9. *Table IV shows how to calculate the number of 4-variable 5-valued functions v-asymmetric functions. The calculation is based on the partitions of* $n = 4$ *into* $r = 5$ *or fewer parts. Since a partition of* $n = 4$ *can have no more than 4 parts, we consider* all *partitions of* $n = 4$*. The second column of Table IV shows all five partitions of* $n = 4$ *in standard form, and the third column shows the exponent form. Here, for example, partition* $4 = 2 + 1 + 1$ *is written as* $2^1 1^2$*. The fourth column shows* one *example assignment of values to the four variables that corresponds to the partition in the second and third column. For example, in the case of partition* $2 + 1 + 1$ *(*$2^1 1^2$*), one assignment is* $(x_1 x_2 x_3 x_4) = 0012$*. That is, 0 is assigned to two variables, 1 is assigned to another variable, and 2 is assigned to the final variable. Indeed, any assignment of values to four variables with two variables the same and a single copy of two different variables could have been chosen as an example. We have chosen, for Table IV, the lexicographically smallest assignment,* 0012 *in this example.*

The fifth column specifies the number of groups of assignments of values to variables that corresponds to a specific choice of values for the variables, according to the partition specified in the second and third column. In the case of partition $2 + 1 + 1(2^1 1^2)$*, there are* $\binom{5}{1}$ *ways to choose the single pair and* $\binom{4}{2}$ *ways to choose the other two values. As shown in the fifth column, this yields a total of* $\binom{5}{1}\binom{4}{2} = 30$ *groups of assignments of variables that corresponds to this partition.*

The sixth column shows how many assignments exist in each group. For the case of our running example, partition $2 + 1 +$

[1]For $n > 2$, $m_n \in \{0, 1\}$, $m_{n-1} \in \{0, 1\}$, ... , and $m_1 \in \{0, 1, 2, \ldots, n\}$.

TABLE IV: Computation of the Number of Maximally v-Asymmetric 4-Variable 5-Valued Functions

Partition Information				# of Grps. of	# of Assgnmnts	A_i/r		Contribution from
i	$n=4$ $r=5$		Example	Assgnmnts G_i	in Each Gr. A_i	Q_i	R_i	Each Partition
1	4	4^1	0000	$\binom{5}{1} = 5$	$\frac{4!}{4!} = 1$	0	1	$\left[\left(\frac{5!}{4!1!}\right)\left(\frac{1!}{0!^4 1!^1}\right)\right]^5 = 2^{11.6}$
2	3+1	$3^1 1^1$	0001	$\binom{5}{1}\binom{4}{1} = 20$	$\frac{4!}{3!1!} = 4$	0	4	$\left[\left(\frac{5!}{1!4!}\right)\left(\frac{4!}{0!^1 1!^4}\right)\right]^{20} = 2^{138.1}$
3	2+2	2^2	0011	$\binom{5}{2} = 10$	$\frac{4!}{2!2!} = 6$	1	1	$\left[\left(\frac{5!}{4!1!}\right)\left(\frac{6!}{1!^4 2!^1}\right)\right]^{10} = 2^{108.1}$
4	2+1+1	$2^1 1^2$	0012	$\binom{5}{1}\binom{4}{2} = 30$	$\frac{4!}{2!1!1!} = 12$	2	2	$\left[\left(\frac{5!}{3!2!}\right)\left(\frac{12!}{2!^3 3!^2}\right)\right]^{30} = 2^{719.6}$
5	1+1+1+1	1^4	0123	$\binom{5}{4} = 5$	$\frac{4!}{1!1!1!1!} = 24$	4	4	$\left[\left(\frac{5!}{1!4!}\right)\left(\frac{24!}{4!^1 5!^4}\right)\right]^5 = 2^{245.7}$
							TOTAL	$1.6592 \times 10^{368} = 2^{1223.2}$

TABLE V: Number Maximally v-/vv-Asymmetric Functions

# of v/vv-Symmetric and Maximally v/vv-Asymmetric Functions									
n	r	#v-S	#vv-S	$\Theta_v(n,r)$	$\Theta_{vv}(n,r)$	**Max=r^n**	# v-Asym	# vv-Asym	r^{r^n}
2	2	$2^{3.0}$	$2^{2.0}$	**1**	**2**	**4**	$2^{3.0}$	$2^{2.0}$	$2^{4.0}$
3	2	$2^{4.0}$	$2^{2.0}$	**2**	**4**	**8**	$2^{7.2}$	$2^{5.3}$	$2^{8.0}$
4	2	$2^{5.0}$	$2^{3.0}$	**7**	**8**	**16**	$2^{11.5}$	$2^{11.5}$	$2^{16.0}$
5	2	$2^{6.0}$	$2^{3.0}$	**14**	**16**	**32**	$2^{26.6}$	$2^{26.5}$	$2^{32.0}$
6	2	$2^{7.0}$	$2^{4.0}$	**30**	**32**	**64**	$2^{55.4}$	$2^{55.6}$	$2^{64.0}$
7	2	$2^{8.0}$	$2^{4.0}$	**60**	**64**	**128**	$2^{119.3}$	$2^{118.3}$	$2^{128.0}$
8	2	$2^{9.0}$	$2^{5.0}$	**127**	**128**	**256**	$2^{236.9}$	$2^{242.3}$	$2^{256.0}$
2	3	$2^{9.5}$	$2^{3.2}$	**3**	**6**	**9**	$2^{12.5}$	$2^{9.1}$	$2^{14.3}$
3	3	$2^{15.8}$	$2^{4.8}$	**16**	**18**	**27**	$2^{26.8}$	$2^{33.1}$	$2^{42.8}$
4	3	$2^{23.8}$	$2^{6.3}$	**48**	**54**	**81**	$2^{100.5}$	$2^{111.3}$	$2^{128.4}$
5	3	$2^{33.3}$	$2^{7.9}$	**153**	**162**	**243**	$2^{338.2}$	$2^{358.6}$	$2^{385.1}$
6	3	$2^{44.4}$	$2^{11.1}$	**483**	**486**	**729**	$2^{1042.9}$	$2^{1112.5}$	$2^{1155.4}$
7	3	$2^{57.1}$	$2^{12.7}$	**1449**	**1458**	**2187**	$2^{3303.4}$	$2^{3407.8}$	$2^{3466.3}$
8	3	$2^{71.3}$	$2^{15.8}$	**4356**	**4374**	**6561**	$2^{10172.8}$	$2^{10316.1}$	$2^{10398.9}$
2	4	$2^{20.0}$	$2^{4.0}$	**6**	**12**	**16**	$2^{29.5}$	$2^{23.1}$	$2^{32.0}$
3	4	$2^{40.0}$	$2^{8.0}$	**40**	**48**	**64**	$2^{103.3}$	$2^{109.9}$	$2^{128.0}$
4	4	$2^{70.0}$	$2^{10.0}$	**186**	**192**	**256**	$2^{386.5}$	$2^{474.7}$	$2^{512.0}$
5	4	$2^{112.0}$	$2^{12.0}$	**744**	**768**	**1024**	$2^{1816.4}$	$2^{1989.0}$	$2^{2048.0}$
6	4	$2^{168.0}$	$2^{18.0}$	**3052**	**3072**	**4096**	$2^{7671.4}$	$2^{8088.2}$	$2^{8192.0}$
7	4	$2^{240.0}$	$2^{22.0}$	**12236**	**12288**	**16384**	$2^{31874.1}$	$2^{32616.7}$	$2^{32768.0}$
8	4	$2^{330.0}$	$2^{30.0}$	**49146**	**49152**	**65536**	$2^{129275.1}$	$2^{130837.6}$	$2^{131072.0}$
2	5	$2^{34.8}$	$2^{4.6}$	**10**	**20**	**25**	$2^{54.8}$	$2^{45.1}$	$2^{58.0}$
3	5	$2^{81.3}$	$2^{7.0}$	**80**	**100**	**125**	$2^{237.9}$	$2^{262.8}$	$2^{290.2}$
4	5	$2^{162.5}$	$2^{11.6}$	**465**	**500**	**625**	$2^{1223.2}$	$2^{1393.1}$	$2^{1451.2}$
5	5	$2^{292.6}$	$2^{16.3}$	**2496**	**2500**	**3125**	$2^{6262.0}$	$2^{7153.3}$	$2^{7256.0}$
6	5	$2^{487.6}$	$2^{23.2}$	**12480**	**12500**	**15625**	$2^{34111.7}$	$2^{36102.6}$	$2^{36280.1}$
7	5	$2^{766.2}$	$2^{30.2}$	**62450**	**62500**	**78125**	$2^{177201.8}$	$2^{181124.3}$	$2^{181400.6}$
8	5	$2^{1149.4}$	$2^{41.8}$	**312400**	**312500**	**390625**	$2^{899435.2}$	$2^{906566.9}$	$2^{907003.2}$
2	6	$2^{54.3}$	$2^{5.2}$	**15**	**30**	**36**	$2^{89.1}$	$2^{75.8}$	$2^{93.1}$
3	6	$2^{144.8}$	$2^{7.8}$	**160**	**180**	**216**	$2^{412.6}$	$2^{521.0}$	$2^{558.4}$
4	6	$2^{325.7}$	$2^{12.9}$	**1065**	**1080**	**1296**	$2^{2555.7}$	$2^{3270.0}$	$2^{3350.1}$
5	6	$2^{651.4}$	$2^{18.1}$	**6440**	**6480**	**7776**	$2^{17903.0}$	$2^{19956.8}$	$2^{20100.7}$
6	6	$2^{1194.3}$	$2^{28.4}$	**38850**	**38880**	**46656**	$2^{114373.1}$	$2^{120337.5}$	$2^{120604.0}$
7	6	$2^{2047.3}$	$2^{36.2}$	**233130**	**233280**	**279936**	$2^{710581.4}$	$2^{723211.7}$	$2^{723624.1}$
8	6	$2^{3326.8}$	$2^{51.7}$	**1399470**	**1399680**	**1679616**	$2^{4315354.7}$	$2^{4341070.8}$	$2^{4341744.4}$

$1(2^1 1^2)$ *corresponds to the number of arrangements specified by the multinomial* $\frac{4!}{2!1!1!} = 12$. *That is, among four variables, there are two of the same type, one of another type, and one of still another type, and this can occur in 12 ways. It specifies how many assignments of variables should all produce the same logic value in a symmetric function, and it is labeled* A_i. *In a maximally v-asymmetric function, the function's value should be distributed uniformly.*

In such a distribution, there are at least $Q_i = \lfloor \frac{12}{5} \rfloor = 2$ *instances of certain function logic values, while* $R_i = 12 - \lfloor \frac{12}{5} \rfloor \times 5 = 2$ *of the function logic values are represented by three logic values. The values of* $Q_i = \lfloor \frac{12}{5} \rfloor = 2$ *and* $R_i = 12 - \lfloor \frac{12}{5} \rfloor \times 5 = 2$ *are shown in the seventh and eighth columns, respectively.*

The rightmost column shows the contribution to the product of contributions of the present partition. As shown, there are $\frac{5!}{3!2!}$ *ways to distribute function logic values so that there is a uniform distribution (two logic values as triples and three as doubles for a total of 5). There are* $\frac{12!}{2!^3 3!^2}$ *assignments in each group. As there are 30 groups, each with* $\frac{5!}{3!2!} \frac{12!}{2!^3 3!^2}$ *ways to assign function values, the contribution of this partition is* $[\frac{5!}{3!2!} \frac{12!}{2!^3 3!^2}]^{30} = 2^{719.6}$. *Now, repeat this computation for the four other partitions, and then compute the product for a total of* $2^{1223.2}$ *functions.* ■

B. vv-Asymmetric Functions

Theorem 7. *The number of* n*-variable* r*-valued vv-asymmetric functions* $N_{vv}(n,r)$ *is*

$$N_{vv}(n,r) = \prod_{i=1}^{p(n,r;n)} \frac{(A_i G_i)!}{(Q_i)!^r}, \tag{13}$$

where A_i *is given by (8),* G_i *is given by (7),* Q_i *is the quotient resulting from the division* $\frac{A_i}{r}$*, and* $p(n,r;n)$ *is the number of partitions on* n *with* r *or fewer parts.*

Proof: This proof is similar to that of Theorem 6. In the case of maximally vv-symmetric functions, for each partition, there is exactly one (large) group of assignments of values to the variables over which the function logic values should be distributed uniformly. For the i-th partition, the size of this group is $A_i G_i$. Further, $A_i G_i$ is divisible by r, and so all uniform distributions are exactly uniform. The number of ways to uniformly distribute the assignments of values to the variables is $(A_i G_i)!/Q_i!^r$. The theorem follows immediately. □

Example 10. *Table VI shows how to calculate the number of 4-variable 5-valued vv-asymmetric functions. The first three columns are identical to the first three columns in Table IV. The remaining columns illustrate the application of (13) in Theorem 7.*

The calculation of the number of maximally vv-asymmetric functions is similar to that of maximally v-asymmetric functions. The difference is in the assignment of variables where the corresponding symmetric function takes on a constant value. In the case of maximally vv-asymmetric functions, the region includes all *assignments corresponding to a single*

TABLE VI: Computation of the Number of Maximally vv-Asymmetric 4-Variable 5-Valued Functions

Partition Information i	$n=4$ $r=5$		Example	# of Grps. of Assgnmnts G_i	# of Assgnmnts in Each Gr. A_i	Total # of Assgnmnts T_i	Q_i	R_i	Contribution from Each Partition
1	4	4^1	0000	$\binom{5}{1} = 5$	$\frac{4!}{4!} = 1$	$5 \cdot 1 = 5$	1	0	$\left(\frac{5!}{5!0!}\right)\left(\frac{5!}{1!^5 2!^0}\right) = 2^{6.9}$
2	3+1	$3^1 1^1$	0001	$\binom{5}{1}\binom{4}{1} = 20$	$\frac{4!}{3!1!} = 4$	$20 \cdot 4 = 80$	16	0	$\left(\frac{5!}{5!0!}\right)\left(\frac{80!}{16!^5 17!^0}\right) = 2^{173.6}$
3	2+2	2^2	0011	$\binom{5}{2} = 10$	$\frac{4!}{2!2!} = 6$	$10 \cdot 6 = 60$	12	0	$\left(\frac{5!}{5!0!}\right)\left(\frac{60!}{12!^5 13!^0}\right) = 2^{128.0}$
4	2+1+1	$2^1 1^2$	0012	$\binom{5}{1}\binom{4}{2} = 30$	$\frac{4!}{2!1!1!} = 12$	$30 \cdot 12 = 360$	72	0	$\left(\frac{5!}{5!0!}\right)\left(\frac{360!}{72!^5 73!^0}\right) = 2^{819.4}$
5	1+1+1+1	1^4	0123	$\binom{5}{4} = 5$	$\frac{4!}{1!1!1!1!} = 24$	$5 \cdot 24 = 120$	24	0	$\left(\frac{5!}{5!0!}\right)\left(\frac{120!}{24!^5 25!^0}\right) = 2^{265.3}$
TOTAL						$(5^4 =)625$			$2.3791 \times 10^{419} = 2^{1393.1}$

partition (beta vector). The column labeled "# of Grps. of Assgnmnts G_i" in Table VI specifies the number of arrangements, and the column labeled "# of Assgnmnts of Each Gr. A_i" specifies the number of ways values can be assigned to arrangements. Their product is the total number of assignments to the variables that should be constant in a vv-symmetric function. This is the same region over which the function logic values should be uniformly distributed. All partitions in Table VI correspond to a region length that is a multiple of $r = 5$. So, a perfectly uniform distribution of assignments of values to variables occurs. In the case of partition $2+1+1$, there are 360 assignments of variables, and the number of ways to achieve a uniform distribution of assignments to function logic values is the multinomial $\frac{360!}{72!72!72!72!72!}$. The right column of Table VI shows the number of distributions for each partition (beta vector). Each can be chosen independently, and so the total number of maximally vv-asymmetric functions is $2^{1393.1}$, a large number. ■

VI. Concluding remarks

Every vv-symmetric function is v-symmetric (e.g., f_2), but not every v-symmetric function is vv-symmetric (e.g., f_1). With respect to v-asymmetric and vv-asymmetric functions, there are v-asymmetric functions that are not vv-asymmetric (e.g., f_3) and vv-asymmetric functions that are not v-asymmetric (e.g., f_4). And, there are functions that are both v-asymmetric and vv-asymmetric (e.g., f_5, which is f_3 with $[0,2,2]^{\mathrm{T}}$ replaced by $[0,1,2]^{\mathrm{T}}$). The Venn diagram in Fig. 2 shows this.

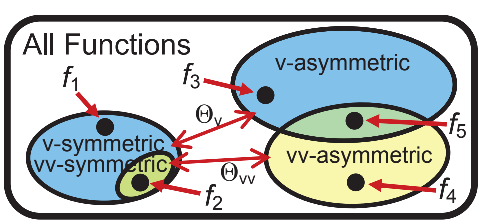

Fig. 2: Venn Diagram of Symmetric/Asymmetric Functions

Although their number was found combinatorially, maximally asymmetric functions seem difficult to quantify. Indeed, in the writing this paper, we were unable to find a maximally asymmetric function with $r > 2$ that would be familiar to the reader. Maximally asymmetric functions tend to resist classification, in the same way that random functions tend to resist classification.

An n-variable maximally asymmetric function has the largest possible asymmetry among all n-variable functions. We consider two types of symmetry, v-symmetric functions which are unchanged by a permutation of the variable labels and vv-symmetric functions, which are unchanged by a permutation of variable labels and variable values. For each, we characterize maximally asymmetric functions, and, from this, enumerate them. There is no similar construction of bent functions. Maximally asymmetric functions tend to be balanced, with function values evenly distributed among the r function values. Thus, they are more like random functions than bent functions.

Acknowledgments

This research is partly supported by a Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research. Three anonymous reviewers provided comments that improved the paper.

References

[1] S. Boztas, R. Hammons, and P. .V. Kumar, "4-Phase sequences with near optimum correlation properties," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1101–1113, May 1992.

[2] A. Bogdonov and A. Rosen, "Pseudorandom functions: Three decades later," in Y. Lindell(ed.) *Tutorials on the Found. of Crypto.*, 2017 Springer Inter. Publ. AG. Part of Springer Nature. pp. 79-158.

[3] J. T. Butler and T. Sasao, "On the properties of multiple-valued functions that are symmetric in both variable values and labels", *28th International Symposium on Multiple-Valued Logic*, May 1998, pp. 83–88.

[4] J. T. Butler and T. Sasao, "An experimental study of asymmetric Boolean functions", *preprint*, 2019.

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

[6] 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*, LNCS 196, pp. 276-288, 1985.

[7] I. Ivchenko, Yu. 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 (2013), 49–63.

[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, Lect. 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 Combonatorial Computing*, November 2018, Vol. 107, pp 181–198.

[11] K, Yang, Y-K Kim, and P. V. Kumar, "Quasi-orthogonal sequences for code-division multiple-access systems", *IEEE Trans. on Infor. Theory*, May 2000, Vol. 46, pp. 982-993.