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 \((r - 1)^{n-1}\).

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, \( 2^{(n-1)} \pm 2^{(\frac{n-1}{2}-1)} \). 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.

II. DEFINITIONS

An \( n \)-variable \( r \)-valued function \( f \) is a mapping from the \( n \) dimensional vector space \( \mathbb{F}_r^n = \{0, 1, \ldots, r - 1\}^n \) into the \( r \)-element field \( \mathbb{F}_r \).

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).

**Example 3.** With $\mathbf{r}$ vector. Each beta vector represents an integer partition on $n$ corresponding beta vector, the lexicographically highest alpha vectors are permutations of each other, there is exactly one that are the next most prolific, etc., and where $\frac{n+r}{2}$ functions $\beta$ function values associated with $f$ function values associated with $f_1$ and $f_2$ from Table I.

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$f_1$</th>
<th>$f_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>1 0 0</td>
<td>0 0</td>
<td>1 0</td>
<td>0 0</td>
</tr>
<tr>
<td>1 1 1</td>
<td>2 0 1</td>
<td>1 1</td>
<td>2 0</td>
<td>1 1</td>
</tr>
<tr>
<td>2 2 2</td>
<td>2 2 0</td>
<td>2 2</td>
<td>2 2</td>
<td>2 2</td>
</tr>
</tbody>
</table>

**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 $\left(\begin{array}{c} n+r+1 \\ 2r+1 \end{array}\right)$ 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 $\nu_v(f)$, is the minimum number of truth table entries that must be changed to convert $f$ to a v-symmetric function; that is,

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

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 $\nu_vv(f)$, is the minimum number of truth table entries that must be changed to convert $f$ to a vv-symmetric function; that is,

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

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 symmetric functions is

$$N_v(n, r) = r \left(\begin{array}{c} n+r-1 \\ r-1 \end{array}\right),$$

(1)

where $\left(\begin{array}{c} n+r-1 \\ r-1 \end{array}\right)$ 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 $\left(\begin{array}{c} n+r-1 \\ r-1 \end{array}\right)$, one for each element of the alpha vector.

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

$$N_{vv}(n, r) = p(n, r; n),$$

(2)

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

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 shows this analytically, as follows.

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

\[
\Theta_{vv}(n, r) = \sum_{i=1}^{p(n, r; n)} \left[ B_i \frac{r - 1}{r} \right],
\]

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 \( \Theta_v \) and \( \Theta_{vv} \), 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, \( \Theta \to \frac{1}{r} r^n \). 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 \( \frac{1}{r} \). When \( n \) is large and \( r \) is fixed, the floor function has negligible effect, and the proportion is close to \( \frac{1}{r} \). 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,

\[
\Theta_v(n, r) \to (r - 1)r^{n-1} \quad \text{and} \quad \Theta_{vv}(n, r) \to (r - 1)r^{n-1},
\]

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 \( 2^n - 2^n/2 - 1 \). 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-Symmetric Functions

Theorem 6. The number of \( n \)-variable \( r \)-valued v-symmetric functions \( N_v(n, r) \) is

\[
N_v(n, r) = \prod_{i=1}^{p(n, r; n)} \frac{r!}{(r - R_i)! R_i!} \frac{A_i!}{(Q_i)(r - R_i)!(R_i + 1)!},
\]

where

\[
G_i = \sum_{i=1}^{p(n, r; n)} \left[ B_i \frac{r - 1}{r} \right],
\]

and \( p(n, r; n) \) is the number of partitions of \( n \) with no more than \( r \) parts.
m specific logic value is assigned to a specific variable, only that to a distinct logic value. The partition does not specify which 1 sets of m each set is assigned to a distinct logic value, there are + m +1 sets of m, corresponding functions are symmetric. So, if the partition is 

Each partition on

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

\[ n^{m_n} (n-1)^{m_{n-1}} \ldots 1^{m_1}, \]  

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 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 \( n: m_n+(n-1): m_{n-1}+\ldots+1: m_1 = n \).

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

\[ L_i = \frac{r!}{(r-R_i)!R_i!}. \]

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

\[ V_i = \frac{A_i!}{Q_i!R_i!(Q_i+1)!}. \]

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

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

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 \( 2^11^2^2 \).

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 (2^11^2^2), 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 (2^11^2^2), 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
TABLE IV: Computation of the Number of Maximally \(v\)-Asymmetric 4-Variable 5-Valued Functions

<table>
<thead>
<tr>
<th>Partition Information</th>
<th>(n = 4)</th>
<th>(r = 5)</th>
<th>Example</th>
<th># of Grps. of Assignments, (G_i)</th>
<th># of Assignments in Each Gr. (A_i/r)</th>
<th>(Q_i/R_i)</th>
<th>Contribution from Each Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>4(^1)</td>
<td>0000</td>
<td>((\binom{4}{1})/4) = 5</td>
<td>(41/24)</td>
<td>0</td>
<td>((\binom{4}{1}/24)^1\times20 = 2^{11.6})</td>
</tr>
<tr>
<td>2</td>
<td>3+1</td>
<td>3(^1)</td>
<td>0001</td>
<td>((\binom{3}{1}/3\times4)^1) = 20</td>
<td>(41/24)</td>
<td>0</td>
<td>((\binom{3}{1}/24)^1\times4 = 2^{13.8})</td>
</tr>
<tr>
<td>3</td>
<td>2+2</td>
<td>2(^2)</td>
<td>0011</td>
<td>((\binom{2}{2}/2\times4)^1) = 10</td>
<td>(41/24)</td>
<td>0</td>
<td>((\binom{2}{2}/24)^1\times1 = 2^{10.8})</td>
</tr>
<tr>
<td>4</td>
<td>2+1+1</td>
<td>2(^1)(^2)</td>
<td>0012</td>
<td>((\binom{2}{1}/2\times4)^1\times10 = 30</td>
<td>(41/24)</td>
<td>0</td>
<td>((\binom{2}{1}/24)^1\times2 = 2^{7.9})</td>
</tr>
<tr>
<td>5</td>
<td>1+1+1+1</td>
<td>1(^4)</td>
<td>0123</td>
<td>((\binom{1}{4}/4\times4)^1) = 5</td>
<td>(41/24)</td>
<td>0</td>
<td>((\binom{1}{4}/24)^1\times4 = 2^{4.5})</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TOTAL = 1.6592 \times 10^{48} = 2^{122.3}</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TABLE V: Number Maximally \(v\)\(-\)\(v\)-Asymmetric Functions

<table>
<thead>
<tr>
<th>(r)</th>
<th>(v)(-v)</th>
<th>(v)(-v) ((n,r,n))</th>
<th>(v)(-v) Symm.</th>
<th>Max N</th>
<th># v-Asymmetric</th>
<th># vv-Asymmetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2()^1) ()^2\</td>
<td>1</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>3</td>
<td>3()^1) ()^2\</td>
<td>4</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>4</td>
<td>4()^1) ()^2\</td>
<td>15</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>5</td>
<td>5()^1) ()^2\</td>
<td>108</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>6</td>
<td>6()^1) ()^2\</td>
<td>540</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>7</td>
<td>7()^1) ()^2\</td>
<td>2700</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>8</td>
<td>8()^1) ()^2\</td>
<td>15120</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>9</td>
<td>9()^1) ()^2\</td>
<td>85040</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
<tr>
<td>10</td>
<td>10()^1) ()^2\</td>
<td>479001</td>
<td>(2\times4)</td>
<td>296</td>
<td>296</td>
<td>296</td>
</tr>
</tbody>
</table>

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

\[N_{vv}(n, r) = \prod_{i=1}^{p(n, r; n)} (A_i G_i)!/(Q_i)^r,\]

where \(A_i\) are given by (8), \(G_i\) is given by (7), \(Q_i\) is the quotient resulting from the division \(A_i\), 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 \(v\)\(-\)\(v\)-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 \(v\)-\(v\)-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 \(v\)-\(v\)-asymmetric functions is similar to that of maximally \(v\)\(-\)\(v\)-symmetric functions. The difference is in the assignment of variables where the corresponding symmetric function takes on a constant value. In the case of maximally \(v\)\(-\)\(v\)-asymmetric functions, the region includes all assignments corresponding to a single column, respectively.

1\(2\()\^2\) corresponds to the number of arrangements specified by the multinomial \(2\times4\)\()^2\ = 12\). 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 \(Q_i = \lfloor \frac{n}{r} \rfloor = 2\) instances of certain function logic values, while \(R_i = 12 - \lfloor \frac{n}{r} \rfloor \times 5 = 2\) of the function logic values are represented by three logic values. The values of \(Q_i = \lfloor \frac{n}{r} \rfloor = 2\) and \(R_i = 12 - \lfloor \frac{n}{r} \rfloor \times 5 = 2\) are shown in the seventh and eighth columns, respectively.
TABLE VI: Computation of the Number of Maximally vv-Asymmetric 4-Variable 5-Valued Functions

<table>
<thead>
<tr>
<th>Partition Information</th>
<th># of Grps. of Assignmats $G_i$</th>
<th># of Assignmats in Each Gr. $A_i$</th>
<th>Total # of Assignmats $T_i$</th>
<th>$Q_i$</th>
<th>$R_i$</th>
<th>Contribution from Each Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>$n = 4$</td>
<td>$r = 5$</td>
<td>Example</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>$4^1$</td>
<td>0000</td>
<td>$\binom{4}{1}$</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>$3+1$</td>
<td>$3^11^1$</td>
<td>0001</td>
<td>$\binom{3}{1}$$\binom{1}{1}$</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>$2+2$</td>
<td>$2^2$</td>
<td>0011</td>
<td>$\binom{2}{2}$</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>$2+1+1$</td>
<td>$2^11^2$</td>
<td>0012</td>
<td>$\binom{2}{1}$$\binom{1}{2}$</td>
<td>30</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>$1+1+1+1$</td>
<td>$1^4$</td>
<td>0123</td>
<td>$\binom{1}{4}$</td>
<td>5</td>
<td>24</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 $[0, 2, 2]^7$ replaced by $[0, 1, 2]^7$. The Venn diagram in Fig. 2 shows this.

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.

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 $[0, 2, 2]^7$ replaced by $[0, 1, 2]^7$. The Venn diagram in Fig. 2 shows this.

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