A Conjunctive Canonical Expansion of Multiple-Valued Functions

Elena Dubrova Petra Färm
Department of Microelectronic and Information Technology
Royal Institute of Technology, Stockholm, Sweden
{elena,petra}@ele.kth.se

Abstract

A generalization of McMillan's conjunctive expansion of Boolean functions [1] to the case of multiple-valued input binary-valued output functions is presented. It is based on the operation of generalized cofactor, defined by employing a new distance measure on truth assignments, called m-valued weighted distance. Using our result, Boolean multiple-output functions can be expanded directly by treating the output part as a single multiple-valued variable. Such an approach might allow a better utilization of the common subparts for different outputs compared to the output-by-output Boolean expansion.

1. Introduction

This paper generalizes McMillan's conjunctive expansion of Boolean functions [1] to the case of multiple-valued input binary-valued output functions $f : M^n \rightarrow \{0,1\}$, $M = \{0, 1, \ldots, m-1\}$. For an n-variable Boolean function, the expansion [1] is a Boolean AND of n components, namely $f = \bigwedge_{i=1}^{n} f_i$. The components f_i, $1 \leq i \leq n$ are defined as $f_i = f^{(i)}|f^{(i-1)}$, where "$|$" is the *generalized cofactor* and $f^{(i)}$ is the *projection* of f onto $(x_1, \ldots, x_i)$, i.e. $f^{(i)} = \exists(x_{i+1}, \ldots, x_n).f$. The generalized cofactor $f^{(i)}|f^{(i-1)}$ agrees with $f^{(i)}$ whenever $f^{(i-1)}$ is true. The minterms for which $f^{(i-1)}$ is false are mapped to the "nearest" minterm where $f^{(i-1)}$ is true, according to the distance measure on truth assignments, defined by

$$d(x,y) = \sum_{i=1}^{n} 2^{n-i} \cdot (x(w_i) \oplus y(w_i)) \qquad (1)$$

where "$\oplus$" is the XOR, "$\sum$" and "$\cdot$" are the arithmetic addition and multiplication, $x, y \in \{0,1\}^n$ are binary vectors and $W = (w_1, \ldots, w_n), w_i \in \{0,1\}$ is a vector of weights. For a fixed W, the nearest minterm is uniquely defined and therefore the expansion $f = \bigwedge_{i=1}^{n} f_i$ is canonical. Note, that if the coefficients 2^{n-i} are omitted in (1), then $d(x,y)$ reduces to the conventional Hamming distance [2].

The main motivation for our generalization is to provide a more efficient way to handle the case of Boolean multiple-output functions. If a k-output Boolean function $\{0,1\}^n \rightarrow \{0,1\}^k$ is treated as a single-output function with one variable being multiple-valued, i.e. of type $\{0,1\}^n \times \{0,1,\ldots,k-1\} \rightarrow \{0,1\}$, then our expansion allows to detect and utilize the common subparts for different outputs directly. Contrary, if the Boolean function is expanded output-by-output, then an additional step might be needed to find the common subparts.

To extend McMillan's conjunctive expansion [1] to the multiple-valued case, we introduced a few notions which might be of interest on their own, namely: (1) a new generalization of Hamming distance $HD(x,y)$ to the case of m-ary vectors $x, y \in M^n$, (2) a definition of weighted distance for m-ary vectors $x, y \in M^n$, (3) an extension of generalized cofactor $f|g$ to the case of $f : M^n \rightarrow M$, $g : M^n \rightarrow \{0,1\}$. To our best knowledge, so far the generalized cofactor has only be extended to the case of $f : M^n \rightarrow \{0,1\}$ and g being a single cube [5].

The paper is organized as follows. Section 2 gives a background on multiple-valued input binary-valued output functions. In Section 3, the generalizations of Hamming distance and weighted Hamming distance between the m-ary vectors are described. In Section 4, the generalized cofactor is extended to the multiple-valued case. In Section 5, a new canonical expansion of multiple-valued functions is introduced. Section 6 concludes the paper.

2. Multiple-valued input binary-valued output functions

This section gives a brief background on multiple-valued input binary-valued output functions. We use the standard definitions and notation in the area of multiple-valued logic [3], [6].

A *multiple-valued input binary-valued output function* is a discrete function of type $f : M^n \rightarrow \{0,1\}$, whose variables range over a finite set of values $M = \{0, 1, \ldots, m-1\}$ and whose output take values from $\{0,1\}$.

Such functions are a "nice" subset of the general multiple-valued functions $M^n \to M$. Many notions and algorithms for the Boolean functions trivially extend to the case of $M^n \to \{0,1\}$. Any multiple-valued input binary-valued output function can be expressed in terms of Boolean AND, Boolean OR and the operation literal of a multiple-valued variable x defined as follows:

$$\overset{S}{x} = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}$$

where $S \subseteq M$ is a subset of constants. Such a representation is possible because the literal is a characteristic function of type $M \to \{0,1\}$ and therefore the operations on the literals are Boolean operations of type $\{0,1\}^n \to \{0,1\}$. It was shown that the set of operations $\{$AND, OR, literals$\}$ is functionally complete for multiple-valued input binary-valued output functions [3].

3. Hamming distance in m-valued case

In this section we extend Hamming distance [2] to the case of m-ary vectors $x, y \in M^n$ and introduce the notion of weighted distance. The later will be used in the next section as a distance measure on truth assignments in the definition of the generalized cofactor.

In the Boolean case, the *Hamming distance* between two binary vectors $x, y \in \{0,1\}^n$ is defined by

$$HD(x,y) = \sum_{i=1}^{n} x(i) \oplus y(i) \tag{2}$$

where " $\oplus$ " is the XOR, " $\sum$ " is the arithmetic addition and $x(i)$ and $y(i)$ are the ith bits of x and y, correspondently. Hamming distance gives the number of position in which two binary vectors differ. For example, $HD(010, 001) = 2$. Two useful properties of Hamming distance are $HD(x,x) = 0$ and $HD(x,y) + HD(y,z) \geq HD(x,z)$, where $x, y, z \in \{0,1\}^n$.

There are several possibilities for extension of Hamming distance to the m-ary vectors, depending on how the XOR between two bits is generalized. One possibility is two extend $x(i) \oplus y(i)$ to the absolute value of the arithmetic subtraction $|x(i) - y(i)|$. For example, for $m = 3$, the difference between 0 and 1 is 1, between 1 and 2 is 1, and between 0 and 2 is 2. Such a definition preserves the properties $HD(x,x) = 0$ and $HD(x,y) + HD(y,z) \geq HD(x,z)$, however it does not allow the unique definition of the "nearest" vector in its weighted extension.

Another possibility is to extend the XOR to the addition modulo m. Then, for $m = 3$, the difference between 0 and 1 is 1, between 1 and 2 is 0, and between 0 and 2 is 2. Since each element of M has a unique inverse with respect to the addition modulo m [3], such a definition guarantees the uniqueness of the "nearest" vector in its weighted extension. However, the properties $HD(x,x) = 0$ and $HD(x,y) + HD(y,z) \geq HD(x,z)$ are not preserved. E.g. $HD(1,1) = 2$ and $HD(0,1) + HD(1,2) = 1 + 0 < HD(0,2) = 2$.

In this paper, we propose an alternative generalization of the XOR, which preserves the properties $HD(x,x) = 0$ and $HD(x,y) + HD(y,z) \geq HD(x,z)$ as well as provides the unique definition of the "nearest" vector in its weighted extension. We generalize the XOR to the bit-wise XOR between m-ary digits $x, y \in M$:

$$x \,\hat{}\, y = \sum_{i=1}^{\lceil logm \rceil} 2^{(\lceil logm \rceil) - i} \cdot (x(i) \oplus y(i)) \tag{3}$$

where " $\oplus$ " is the XOR, " $\sum$ " and " $\cdot$ " are the arithmetic addition and multiplication and $x(i)$ and $y(i)$ are the ith bits of x and y, correspondently.

Note, that " $\hat{}$ " is the operation of type $M^2 \to \{0, 1, \ldots, 2^{\lceil logm \rceil} - 1\}$, so, unless m is of type 2^k for some $k \geq 1$, " $\hat{}$ " has more than m values in its output domain. For example, for $m = 3$, the output domain of " $\hat{}$ " is $\{0,1,2,3\}$, e.g. $2 \,\hat{}\, 2 = 0$, $0 \,\hat{}\, 1 = 1$, $0 \,\hat{}\, 2 = 2$ and $1 \,\hat{}\, 2 = 3$. Using this extension of the XOR, our generalization of Hamming distance is as follows.

Definition 1 *The m-valued distance between the two m-ary vectors $x, y \in M^n$ is defined by*

$$d_m(x,y) = \sum_{i=1}^{n} x(i) \,\hat{}\, y(i) \tag{4}$$

where " $\hat{}$ " is defined by (3), " $\sum$ " is the arithmetic addition, and $x(i)$ and $y(i)$ are the ith digits of x and y, correspondently.

Note, that in the above definition $x(i)$ and $y(i)$ are ith *digits*, not bits. For example, in the ternary vector $x = (210)$, the 1st digit is 2, the 2nd is 1 and the 3rd is 0. So, the distance between the vectors (210) and (021) is $d_m(210, 021) = 2 + 3 + 1 = 6$. Using the properties of the " $\hat{}$ ", we can easily show that the m-valued distance defined by (4) satisfies the properties $d_m(x,x) = 0$ and $d_m(x,y) + d_m(y,z) \geq d_m(x,z)$, where $x, y, z \in M^n$.

Next, we extend the Definition 1 to its weighted version.

Definition 2 *Given a weight vector $W = (w_1, \ldots, w_n)$, $w_i \in M$, the m-valued weighted distance between the two m-ary vectors $x, y \in M^n$ is defined by*

$$wd_m(x,y) = \sum_{i=1}^{n} (2^{\lceil logm \rceil})^{n-i} \cdot (x(w_i) \,\hat{}\, y(w_i)) \tag{5}$$

where " $\hat{}$ " is defined by (3), " $\sum$ " and " $\cdot$ " are the arithmetic addition and multiplication, and $x(w_i)$ and $y(w_i)$ are the ith digits of x and y, correspondently.

For $m = 2$, the coefficient $2^{\lceil logm \rceil}$ in (5) reduces to 2, which agrees with the definition of weighted Boolean difference (1).

From the number representation theory, we know that a vector of digits $(a_{n-1} \dots a_0)$, $a_i \in \{0, 1, \dots, k-1\}$ over a radix r represents the number [3]:

$$a_{n-1}r^{n-1} + a_{n-2}r^{n-2} + \dots + a_0.$$

If $r \geq k$, then the above representation is unique. Otherwise, it is redundant, i.e. different vectors can represent the same number. In our case, $a_i = x(w_i) \,\hat{}\, y(w_i) \in \{0, 1, \dots, 2^{\lceil logm \rceil} - 1\}$ and $r = 2^{\lceil logm \rceil}$, so our representation is unique as long as for any m-ary digits $x, y, z \in M$ it holds that $x \,\hat{}\, y = x \,\hat{}\, z$ if and only if $y = z$ (cancellation law of addition). This clearly holds for "$\hat{}$". Therefore, given a fixed weight vector $W = (w_1, \dots, w_n)$, the distance (5) uniquely defines the nearest vector for any m-ary vector from M^n.

For example, for $m = 3$, $n = 3$ and $W = (1, 2, 3)$ the nearest point to (021) is (020), yielding the minimal distance $wd_m(021, 020) = (0 \,\hat{}\, 0) \cdot 4^2 + (2 \,\hat{}\, 2) \cdot 4^1 + (1 \,\hat{}\, 0) \cdot 4^0 = 1$. For $W = (2, 3, 1)$, the nearest point to (021) is (001), yielding the minimal distance $wd_m(021, 001) = (1 \,\hat{}\, 1) \cdot 4^2 + (0 \,\hat{}\, 0) \cdot 4^1 + (2 \,\hat{}\, 0) \cdot 4^0 = 2$. This uniqueness property of the m-valued weighted distance is used in the next section as a distance measure on truth assignments in the definition of the generalized cofactor.

4. Generalized cofactor

If f and g are n-variable Boolean functions, then the generalized cofactor $f|g$ is a Boolean function which value for a given minterm $x \in \{0, 1\}^n$ is obtained by finding the nearest minterm $y \in \{0, 1\}^n$ that satisfies g, and evaluating f at this point [1]. The nearest minterm is defined as the one minimizing $d(x, y)$ (1) for a given W. Such a definition of the generalized cofactor coincides with the definition of the *constrain* operator on OBDD's [4] in the special case when the OBDD variable order is W.

The definition of the generalized cofactor from [1] directly extends to the case of $f : M^n \to M$, $g : M^n \to \{0, 1\}$ if the m-valued weighted distance $wd_m(x, y)$ is used instead of Boolean weighted difference (1) as a distance measure on truth assignments. Let $\mathbf{0}$ denote the constant-0 function.

Definition 3 *For a minterm $x \in M^n$ and a function $g : M^n \to \{0, 1\}$ such that $g \neq \mathbf{0}$, let $x \to g$ be the minterm $y \in M^n$ for which $g(y) = 1$ and $wd_m(x, y)$ is minimized.*

So, $x \to g$ is the nearest point to x which satisfies g. As we showed in the last section, $x \to g$ is uniquely defined for $x \in M^n$. Clearly, if x satisfies g itself, i.e. if $g(x) = 1$, then $x \to g = x$, since $wd_m(x, x) = 0$ is the minimal possible distance. This implies that $f|g$ agrees with f for every minterm x satisfying g.

Definition 4 *For any functions $f : M^n \to M$ and $g : M^n \to \{0, 1\}$, the generalized cofactor $f|g$ is a function of type $M^n \to M$ defined as follows:*
- if $g \neq \mathbf{0}$, then $f|g(x) = f(x \to g)$ for any $x \in M^n$,
- else $f|g = \mathbf{0}$.

A number of properties of Boolean generalized cofactor from [1] hold for the multiple-valued case. For example, it is easy to show that if g is a literal, then the generalized cofactor reduces to the conventional cofactor over a variable:

$$f| \overset{j}{x_i} = f|_{x_i = j}$$

where $f|_{x_i = j} = f(x_1, \dots, x_{i-1}, j, x_{i+1}, \dots, x_n)$.

If g is a cube C and f is of type $f : M^n \to M$, then the generalized cofactor coincides with the cofactor over a cube $f|_C$ from [5]. It is interesting to observe that in this case the generalized cofactor is independent of the weight vector W.

As an example, consider the case of $m = 3$, $n = 2$ and $W = (w_1, w_2)$. The generalized cofactor of a function $f = \overset{0,1}{x_1}\overset{0}{x_2}$ with respect to $g = \overset{0}{x_1}\overset{0,1}{x_2}$ is $f|g = \overset{0,2}{x_2}$. If $f = \overset{0,1}{x_1}\overset{0}{x_2} + \overset{0,2}{x_1}\overset{1}{x_2} + \overset{1,2}{x_1}\overset{2}{x_2}$, and $g = \overset{0}{x_1}\overset{0,1}{x_2} + \overset{1}{x_1}\overset{1}{x_2}$, then we get $f|g = \overset{0,2}{x_1}$.

5. Conjunctive expansion

Similarly to the Boolean case, we use the generalized cofactor to decompose a multiple-valued input binary-valued output function $f : M^n \to \{0, 1\}$ into a Boolean AND of n multiple-valued input binary-valued output functions $f_1, \dots, f_n$, defined as follows.

Definition 5 *For any $f : M^n \to \{0, 1\}$ and $1 \leq i \leq n$,*

$$f_i = f^{(i)} | f^{(i-1)}$$

where $f^{(i)}$ stands for the projection of f onto $(x_1, \dots, x_i)$, i.e. $f^{(i)} = \exists (x_{i+1}, \dots, x_n).f$.

The proof of definition 5 is based on the following Lemma:

Lemma 1 *If f and g are of type $M^n \to \{0, 1\}$, then*

$$(f|g) \cdot g = f \cdot g$$

where "$\cdot$" is the Boolean AND.

Proof: By Definition 3, $(f|g)(x) = f(x)$ for every minterm $x \in M^n$ where $g(x) = 1$. So, we get $(f|g)(x) \cdot g(x) = f(x) \cdot g(x) = f(x)$ on the left hand side and $f(x) \cdot g(x) = f(x)$ on the right hand side.

On the other hand, for any $x \in M^n$ such that $g(x) = 0$, we have $(f \cdot g)(x) = 0$ on the right hand side and $(f|g)(x) \cdot g(x) = 0$ on the left hand side.

$\square$

Theorem 1 *Any multiple-valued input binary-valued output function $f : M^n \to \{0,1\}$ can be expressed as*

$$f = \bigwedge_{i=1}^{n} f_i \tag{6}$$

where " $\bigwedge$ " is the Boolean AND.

Proof: (same as in [1]) By induction on n.
1) Let $n = 1$. Then $f = f_1 = f^{(1)}|f^{(0)} = f^{(1)}|\mathbf{1} = f^{(1)} = f$, where **1** denotes the constant-1 function.
2) Hypothesis: Assume the result for all functions of n variables.

$$\begin{aligned} \bigwedge_{i=1}^{n+1} f_i &= (\bigwedge_{i=1}^{n} f_i) \cdot f_{n+1} \\ &= f^{(n)} \cdot (f^{(n+1)}|f^{(n)}) \\ &= f^{(n)} \cdot f^{(n+1)} \\ &= f^{(n+1)}. \end{aligned}$$

$\square$

The expansion (6) is canonical for a fixed weight vector $W = (w_1, \ldots, w_n), w_i \in M$. Similarly to the Boolean case [1], if a function f does not depend on some variable x_i, then $f^{(i)} = f^{(i-1)}$. Therefore $f_i = f^{(i)}|f^{(i)} = \mathbf{1}$, so the corresponding component f_i in (6) is constant-1.

As an example of the application of the expansion (6) to multiple-output Boolean functions, consider the 2-output 4-variable Boolean function with $f(out_1) = x_1'x_2'x_3'x_4' + x_1'x_2x_3'x_4 + x_1x_2x_3x_4 + x_1x_2'x_3x_4'$ and $f(out_2) = x_1'x_2'x_3x_4' + x_1'x_2x_3x_4 + x_1x_2x_3'x_4 + x_1x_2'x_3'x_4'$. We treat its output part as a single variable x_5 (2-valued in this case) and represent it as a 5-variable function $f = f(out_1) \cdot x_5' + f(out_2) \cdot x_5$. By applying (6) to f, we get $f = \bigwedge_{i=1}^{5} f_i$ with $f_1 = f_2 = f_3 = \mathbf{1}$, $f_4 = x_2x_4 + x_2'x_4'$ and $f_5 = x_1'x_3'x_5' + x_1x_3x_5' + x_1'x_3x_5 + x_1x_3'x_5$. So, $f = f_4 \cdot f_5$ with 6 products in the decomposed representation versus 8 in the non-decomposed.

If instead of using multiple-valued expansion, we apply the Boolean one output-by-output, then we get $f(out_1) = f_3(out_1) \cdot f_4(out_1)$ with $f_4(out_1) = x_2x_4 + x_2'x_4'$ and $f_5(out_1) = x_1'x_3'x_5' + x_1x_3x_5'$ and $f(out_2) = f_3(out_2) \cdot f_4(out_2)$ with $f_4(out_2) = x_2x_4 + x_2'x_4'$ and $f_5(out_2) = x_1'x_3'x_5 + x_1x_3x_5$. An additional step is needed to recognize that $f_4(out_1) = f_4(out_2)$.

6. Conclusion

This paper extends McMillan's conjunctive expansion of Boolean functions [1] to the multiple-valued case. Although the generalization is done only for the case of multiple-valued input binary-valued output functions, the more general case of $f : M^n \to M$ can also be handled by first partitioning f with respect to each of its non-zero values $i \in M - \{0\}$ into $m-1$ literals $\overset{i}{f}: M^n \to \{0,1\}$, and then expanding each of $\overset{i}{f}$. The resulting expansion for f is of type

$$f = \sum_{i=1}^{m-1} (i \cdot \bigwedge_{j=1}^{n} \overset{i}{f}_j)$$

where " $\sum$ " and " $\cdot$ " are the multiple-valued operations maximum and minimum, correspondently.

It is worth noticing that the variable ordering in the weight vector W might considerably impact the size of the expansion (6). The problem of finding an optimal variable ordering is still open in both the Boolean as well as the multiple-valued case.

Acknowledgment

This work was supported in part by Vinnova EXCITE project N^{Ω} 6472 and by IBM Faculty Award.

References

[1] K.L. McMillan, A conjunctively decomposed boolean representation for symbolic model checking, *Computer Aided Verification: 8th Int. Conf. (CAV'96)*, R. Alur and T. Henzinger eds., New Brunswick, New Jersey, July 1996.

[2] R. W. Hamming, Error detecting and error correcting codes, *Bell System technical Journal*, vol. 26, no. 2, pp. 147-160, April 1950.

[3] J.C. Muzio, T.C. Wesselkamper, *Multiple-Valued Switching Theory*, Adam Hilger Ltd. Bristol and Boston, 1986.

[4] O. Coudert, C. Berthet, J.C. Madre, Verification of synchronous sequential machines based on symbolic execution, in J. Sifakis, ed., *Int. Workshop on Automatic Verification Methods for Finite State Systems*, Grenoble, France, vol. 407 of Lecture Notes in Computer Science, Springer-Verlag, June 1989.

[5] R. Rudel and A. Sangiovanni-Vincentelli, Multiple-valued minimization for PLA optimization, *IEEE Trans. on CAD/ICAS*, vol. CAD-5, no. 9, pp. 727-750, Sept. 1987.

[6] S. Hassoun and T. Sasao, eds., *Logic Synthesis and Verification*, Kluwer Academic Publishers, 2002.