УДК 517.98

Т.В. Авлочинская, П.Н. Бибило

Экспериментальное исследование разделимости частичных булевых функций на основе решения логических уравнений

Описаны результаты экспериментального исследования алгоритма декомпозиции частичных булевых функций и систем, основанного на сведении задачи декомпозиции к задаче «выполнимость конъюнктивной нормальной формы». Для проверки выполнимости задачи использованы известные *SAT*-программы *picosat* и *zChaff*.

The results of experimental research of the decomposition algorithm for partial Boolean functions and systems are described. The algorithm is based on the reduction of the decomposition problem to the SAT problem. To check the satisfiability for the given CNF the SAT-programmes (picosat and zChaff) are used.

Описано результати експериментального дослідження алгоритму декомпозиції часткових булевих функцій і систем, заснованого на зведенні задачі декомпозиції до задачі «виконуваності кон'юнктивної нормальної форми». Для перевірки виконуваності задачи використано відомі *SAT*-програми *picosat* та *zChaff*.

Введение Задача разделения (декомпозиции) булевой функции на подфункции давно изучается в литературе с целью создания эффективных методов синтеза комбинационных логических схем в различных технологических базисах. В настоящее время декомпозиция находит практическое применение при синтезе структур *FPGA* (*Field-Programmable Gate Arrays*) [1], получивших широкое распространение при реализации цифровых схем. В литературе проведена классификация видов разложений булевых функций, сформулированы критерии существования разложений функций и систем функций, предложены методы, алгоритмы и программы декомпозиции. Проблемам декомпозиции посвящен обзор [2] и монографии [3–5]. При решении задач декомпозиции используются различные формальные модели – булевы и троичные матрицы [6], специальные таблицы [5], аппарат понятий производной, дифференциала и разности булевой функции [7], спектральные представления [8] и др. Предлагается также [5, 9] использовать логические уравнения и преобразовывать уравнения к виду конъюнктивной нормальной формы (КНФ), т.е. сводить решение задачи декомпозиции к задаче выполнимости КНФ (*Boolean satisfiability problem – SAT-problem*) [10]. Для решения КНФ-уравнений имеются мощные *SAT*-программы (*SAT-solvers*) [11], хорошо зарекомендовавшие себя при верификации логических схем [12].

В статье описаны результаты экспериментального исследования свойства разделимости (декомпозабельности) не полностью определенных булевых функций и систем в зависимости от степени определенности функций, числа функций в системе и других параметров. Для проверки существования функциональных разложений используется аппарат логических уравнений, для решения уравнений – известные *SAT*-программы *picosat* и *zChaff* [11].

Основные понятия и определения

Булевыми называются двоичные (0, 1) функции $f(\underline{x}) = f(x_1, x_2, \ldots, x_n)$ двоичных (булевых) переменных $x_1, x_2, \ldots, x_n$. Пусть V^x – булево пространство, построенное над переменными булева вектора $\underline{x} = (x_1, x_2, \ldots, x_n)$. Элементами этого пространства являются n-компонентные наборы (векторы) $\underline{x}^*$ нулей и единиц. Булева функция, значения 0, 1 которой определены на всех 2^n элементах $\underline{x}^* \in V^x$, называется *полностью определенной*. Если же на некоторых элементах булева пространства V^x значения функции не определены, то такая функция называется не полностью определенной или *частичной*. Частичная булева функция принимает единичное значение на элементах $\underline{x}^*$ подмножества M_f^1 булева пространства V^x и нулевое значение на элементах подмножества M_f^0. На всех остальных элементах пространства V^x, образующих подмножество M_f^- пространства V^x, значение частичной функции не определено. Очевидно, что $M_f^0 \cup M_f^1 \cup \cup M_f^- = V^x$, а $\left|M_f^0\right| + \left|M_f^1\right| + \left|M_f^-\right| = 2^n$, где через

$|M|$ обозначена мощность множества M. Под *степенью неопределенности* d булевой функции будем понимать отношение мощности множества M_f^- к мощности всего булева пространства V^x, т.е. $d = \dfrac{|M_f^-|}{2^n}$. *Степень определенности* s частичной булевой функции выражается суммой $s = s^0 + s^1$ величин $s^0 = \dfrac{|M_f^0|}{2^n}$, $s^1 = \dfrac{|M_f^1|}{2^n}$.

Пример частичной булевой функции, зависящей от переменных x_1, x_2, x_3, x_4, x_5, приведен в табл. 1. Для данной функции $s^0 = s^1 = 5/32$, $s = 10/32$, $d = 22/32$. Упорядоченную систему частичных булевых функций будем называть далее частичной векторной булевой функцией или просто *векторной* функцией.

Пусть задана частичная функция $f(x_1, \ldots, x_n) = f(\underline{x})$ и разбиение множества $X = \{x_1, \ldots, x_n\}$ ее аргументов на два непересекающиеся подмножества $Y = \{y_1, \ldots, y_r\}$, $Z = \{z_1, \ldots, z_{n-r}\}$.

Разделением (*декомпозицией*) частичной булевой функции $f(\underline{x})$ по двухблочному разбиению Y, Z множества аргументов X называется процесс представления $f(\underline{x})$ в виде суперпозиции (функционального разложения)

$$f(\underline{x}) = f(\underline{y}, \underline{z}) = g(\underline{h}(\underline{y}), \underline{z}), \qquad (1)$$

где $g(\underline{h}(\underline{y}), \underline{z})$ – частичная булева функция, $\underline{h}(\underline{y}) = h_1(\underline{y}), \ldots, h_p(\underline{y}))$ – частичная векторная функция.

Сведение задачи декомпозиции к решению логического уравнения

Проиллюстрируем известное [5] сведение задачи многократной декомпозиции к решению логического уравнения на примере декомпозиции частичной функции $f(x_1, x_2, x_3, x_4, x_5)$ (табл. 1) по разбиению $Y = \{x_1, x_2, x_3\}$, $Z = \{x_4, x_5\}$ множества переменных $X = \{x_1, x_2, x_3, x_4, x_5\}$.

Этап 1. Найдем коэффициенты разложения Шеннона частичной булевой функции $f(x_1, x_2, x_3, x_4, x_5)$ по подмножеству $Y = \{x_1, x_2, x_3\}$ и зададим их в табл. 2.

Построим граф G (рис. 1) отношения несовместимости на множестве векторов $\underline{y}_i^* \in V^y$, используя полученные коэффициенты. Например, в этом графе G имеется ребро между вершинами 000, 001, так как коэффициенты $f_{000}\, f_{001}$ не могут быть доопределены до одной функции – имеется набор $\underline{z} = (00)$, на котором $f_{000}(00) = 0$, а $f_{001}(00) = 1$. Вершины 000, 010 не соединены ребром (являются несмежными), так как соответствующие им коэффициенты f_{000}, f_{010} могут быть доопределены до одной и той же функции, в качестве такой функции может быть функция f_{000}.

Таблица 1

$\underline{x}$	F	Область значений
00000	0	M_f^0
00011	0	
01000	0	
01101	0	
01110	0	
00001	1	M_f^1
00100	1	
00110	1	
00111	1	
01001	1	
00010	–	M_f^-
00101	–	
01010	–	
01011	–	
01100	–	
01111	–	
10000	–	
10001	–	
10010	–	
10011	–	
10100	–	
10101	–	
10110	–	
10111	–	
11000	–	
11001	–	
11010	–	
11011	–	
11100	–	
11101	–	
11110	–	
11111	–	

Таблица 2

$\underline{z} = (x_4, x_5)$	f_{000}	f_{001}	f_{010}	f_{011}	f_{100}	f_{101}	f_{110}	f_{111}
00	0	1	0	–	–	–	–	–
01	1	–	1	0	–	–	–	–
10	–	1	–	0	–	–	–	–
11	0	1	–	–	–	–	–	–

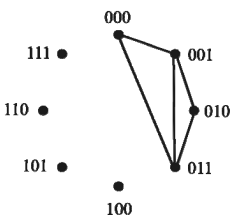

Рис. 1. Граф G отношения несовместимости

Минимальное число $p_{\min}$ промежуточных функций $h_i(\underline{y})$ в многократном разложении (1) частичной функции $f(x)$ определяется из соотношения

$$p_{\min} =]\log_2 \chi(G)[, \qquad (2)$$

где $\chi(G)$ – хроматическое число графа G, через $]a[$ обозначено ближайшее сверху целое число, большее либо равное a. Если граф G не содержит ребер (является пустым), то подмножество Y является несущественным ($p_{\min} = 0$) подмножеством аргументов функции $f(\underline{x})$.

При построении разложения (1) возникает вопрос о нетривиальности полученного решения.

Утверждение 1. Условия $p < r$, $n - r > \log_2 p$ выделяют класс нетривиальных многократных разложений (1).

При условии $p \geq r$ в получившемся разложении нет уменьшения числа компонент вектора $\underline{y}$ в сравнении с числом p компонент вектора $\underline{h}(\underline{y})$. Так как число k всех возможных коэффициентов разложения Шеннона по подмножеству Y ограничено неравенством $k \leq 2^{2^{n-r}}$, а для существования разложения (1) необходимо не более 2^p различных дизъюнктивных членов [2], то $2^p \leq 2^{2^{n-r}}$, откуда $n - r > \log_2 p$.

Далее под *свойством разделимости функции* по заданному разбиению Y, Z множества ее аргументов будем понимать свойство функции иметь нетривиальное разложение вида (1).

В рассматриваемом примере граф G является 3-хроматическим ($\chi(G) = 3$), а минимальное число промежуточных функций равно двум: $]\log_2 \chi(G)[= 2$ и $\underline{h} = (h_1, h_2)$.

Этап 2. Составление логического уравнения для заданного числа $p = 2$ промежуточных функций. Закодируем неизолированные вершины булевыми переменными w_i так, как дано в табл. 3.

Таблица 3

Вершина графа G	Код вершины	Решение 1	Решение 2
		$h_1 h_2$	$h_1 h_2$
000	$w_1\, w_2$	1-	01
001	$w_3\, w_4$	00	11
010	$w_5\, w_6$	10	0-
011	$w_7\, w_8$	01	10

Запишем логическое уравнение, выражающее условия существования решения – условия существования частичной векторной функции $\underline{h} = (h_1, h_2)$, принимающей ортогональные значения для каждой пары смежных вершин графа G [5]. Например, для пары 000, 001 смежных вершин графа G значения функции будут ортогональными тогда и только тогда, когда логическое уравнение

$$(w_1 \oplus w_2) \vee (w_3 \oplus w_4) = 1$$

будет иметь решение. Для того чтобы найти функцию $\underline{h} = (h_1, h_2)$, удовлетворяющую подобным условиям по всем ребрам графа G, требуется решить логическое уравнение

$$((w_1 \oplus w_3) \vee (w_2 \oplus w_4)) \,\&\, ((w_1 \oplus w_7) \vee$$
$$\vee (w_2 \oplus w_8)) \,\&\, (w_3 \oplus w_5) \vee (w_4 \oplus w_6)) \,\&$$
$$\&\, ((w_3 \oplus w_7) \vee (w_4 \oplus w_8)) \,\&\, ((w_5 \oplus w_7) \vee$$
$$\vee (w_6 \oplus w_8)) = 1, \qquad (3)$$

составленное по всем ребрам графа G.

Каждый конъюнктивный член уравнения может быть записан в виде КНФ, после чего уравнение (3) приобретает вид КНФ

$$(\overline{w_1} \vee \overline{w_2} \vee \overline{w_3} \vee \overline{w_4}) \,\&\, (w_1 \vee \overline{w_2} \vee w_3 \vee \overline{w_4}) \,\&$$
$$\&\, (\overline{w_1} \vee w_2 \vee \overline{w_3} \vee w_4) \,\&\, (w_1 \vee w_2 \vee w_3 \vee w_4) \,\&$$
$$\&\, (\overline{w_1} \vee \overline{w_2} \vee \overline{w_7} \vee \overline{w_8}) \,\&\, (w_1 \vee \overline{w_2} \vee w_7 \vee \overline{w_8}) \,\&$$
$$\&\, (\overline{w_1} \vee w_2 \vee \overline{w_7} \vee w_8) \,\&\, (w_1 \vee w_2 \vee w_7 \vee w_8) \,\&$$
$$\&\, (\overline{w_3} \vee \overline{w_4} \vee \overline{w_5} \vee \overline{w_6}) \,\&\, (w_3 \vee \overline{w_4} \vee w_5 \vee \overline{w_6}) \,\&$$
$$\&\, (\overline{w_3} \vee w_4 \vee \overline{w_5} \vee w_6) \,\&\, (w_3 \vee w_4 \vee w_5 \vee w_6) \,\&$$
$$\&\, (\overline{w_3} \vee \overline{w_4} \vee \overline{w_7} \vee \overline{w_8}) \,\&\, (w_3 \vee \overline{w_4} \vee w_7 \vee \overline{w_8}) \,\&$$
$$\&\, (\overline{w_3} \vee w_4 \vee \overline{w_7} \vee w_8) \,\&\, (w_3 \vee w_4 \vee w_7 \vee w_8) \,\&$$
$$\&\, (\overline{w_5} \vee \overline{w_6} \vee \overline{w_7} \vee \overline{w_8}) \,\&\, (w_5 \vee \overline{w_6} \vee w_7 \vee \overline{w_8}) \,\&$$
$$\&\, (\overline{w_5} \vee w_6 \vee \overline{w_7} \vee w_8) \,\&\, (w_5 \vee w_6 \vee w_7 \vee w_8) = 1. \qquad (4)$$

Данное уравнение имеет решения, два из них приведены в табл. 3. На данном примере продемонстрировано, каким образом проверка существования разложения (1) с заданным числом p промежуточных функций может быть сведена к составлению КНФ-уравнения вида (4) и нахождению его решений, т.е. к решению задачи о выполнимости КНФ. После того, как векторная функция $\underline{h}(\underline{y}) = (h_1(\underline{y}), ..., h_p(\underline{y}))$ най-

дена, построение частичной функции $g(\underline{h}(\underline{y}),\underline{z})$ не вызывает затруднений и описано в [5]. В результате строится частичная булева функция $g(\underline{h}(\underline{y}),\underline{z})$, *реализующая* частичную булеву функцию $f(\underline{x})$. Если говорить более строго, равенство $f(\underline{y},\underline{z}) = g(\underline{h}(\underline{y}),\underline{z})$ – отношение реализации частичных булевых функций.

Пусть L – число дуг, инцидентных той вершине графа G, которая имеет максимальную степень. Если при составлении логического уравнения начальное значение числа p определяется по формуле

$$p = \rceil \log_2 L \lceil \qquad (5)$$

и логическое уравнение составляется только один раз, то такая оценка разделимости (нахождение минимального значения числа p) является приближенной. Далее будем называть основанный на данной оценке алгоритм ***быстрым алгоритмом*** оценки разделимости.

Точный алгоритм оценки разделимости, т.е. нахождения минимального значения числа p, начинает свою работу, используя формулу (5), и если логическое уравнение имеет решение для такого значения p, то число p уменьшается на единицу. Для меньшего значения p составляется и решается новое логическое уравнение и т.д. Если для p уравнение имеет решение, а для $p-1$ решений уравнения не существует, то $p = p_{\min}$.

Программная реализация. Выбор *SAT*-программ

Для написания программного комплекса «Декомпозиция булевых функций» использовались следующие технологии разработки программного обеспечения:

- *Java Development Kit* 1.6 (*JRE* 1.6).
- Библиотека для *JUnit*-тестов: *junit*-4.5.jar.
- Язык сценариев для *Batch* файлов.

При разработке использовалась интегрированная среда разработки *java*-приложений *NetBeans IDE* 6.8. Выбор технологии осуществлялся по принципу выгодного соотношения производительности языка программирования и скорости разработки. Язык программирования *Java* дает хорошую возможность построить удобную ООП-модель классов, на основе которой и были реализованы алгоритмы декомпозиции.

Для решения задачи выполнимости КНФ выбраны *SAT*-программы picosat и *zChaff* [11]. Данные программы написаны на языке *C++*, находятся в свободном доступе и используют текстовый формат *.cnf* для представления входных данных. В результате своей работы *SAT*-программы выдают либо ответ о том, что КНФ невыполнима (не имеет решения), либо ответ о том, что КНФ выполнима – в этом случае выдается хотя бы одно решение. Выбранные *SAT*-программы имеют очень высокие показатели производительности: программа *picosat* заняла второе место на соревнованиях *SAT*-программ в 2007 году, *zChaff* – первое место на соревнованиях *SAT*-программ в 2004 году, способна обрабатывать КНФ, состоящие из 10 миллионов дизъюнктов [9].

Организация экспериментов

Цель экспериментов – изучение свойства разделимости псевдослучайных частичных булевых функций и систем таких функций в зависимости от степени определенности (неопределенности) функций, мощности перекодируемого подмножества Y аргументов, числа m функций в системе и других параметров.

Для генерации псевдослучайной частичной булевой функции требуется указать число n аргументов функции и числа $v_0 = \left| M_f^0 \right|$, $v_1 = \left| M_f^1 \right|$. Получение псевдослучайной (далее – случайной) частичной функции осуществляется генерацией $v_0 + v_1$ различных псевдослучайных чисел (n–разрядных двоичных наборов), первые v_0 из которых интерпретируется как область M_f^0 нулевых значений функции, следующие v_1 наборов – как область M_f^1 единичных значений функции. Выбор подмножества Y перекодируемых аргументов заданной мощности r осуществлялся *случайным* образом. Проверка существования разложения (1) сводилась к построению логического уравнения в текстовом формате *.cnf*, являющемся исходным для программ *picosat*, *zChaff* решения задачи «выполнимость КНФ».

Например, уравнение (4) – исходные данные для программы *picosat* – записывается в виде

```
p cnf 8 20
-1  -2  -3  -4  0
 1  -2   3  -4  0
-1   2  -3   4  0
 1   2   3   4  0
-1  -2  -7  -8  0
 1  -2   7  -8  0
-1   2  -7   8  0
 1   2   7   8  0
-3  -4  -5  -6  0
 3  -4   5  -6  0
-3   4  -5   6  0
 3   4   5   6  0
-3  -4  -7  -8  0
 3  -4   7  -8  0
-3   4  -7   8  0
 3   4   7   8  0
-5  -6  -7  -8  0
 5  -6   7  -8  0
-5   2  -7   8  0
 5   2   7   8  0
0
```

В такой записи каждая строка (кроме первой и последней) задает один дизъюнкт, знак минус свидетельствует об инверсном литерале, например, строка

```
-1 -2 -3 -4 0
```

соответствует первому дизъюнкту

$$(\overline{w}_1 \vee \overline{w}_2 \vee \overline{w}_3 \vee \overline{w}_4)$$

в формуле (4). Символ 0 в последней строке указывает на окончание записи КНФ, в первой строке: число 8 – это число переменных КНФ, 20 – это число дизъюнктов в КНФ (4).

Экспериментальные исследования

Эксперимент 1. Как влияет степень неопределенности на разделимость функции?

В данном эксперименте генерировалось 100 псевдослучайных булевых функций для каждого значения параметра n (числа аргументов) и d (степени неопределенности), причем полагалось $s^1 = s^0$. Для каждой из функций случайным образом выбиралось r перекодируемых аргументов (множество Y), затем составлялись логические уравнения и находились минимальные числа $p_{\min}$ промежуточных функций в разложениях (1), осуществлялась проверка нетривиальности полученных разложений. Полученные по 100 функциям значения $p_{\min}$ усреднялись, подсчитывалась доля R (процент) функций, для которых получались нетривиальные разложения. Результаты эксперимента 1 для *быстрого алгоритма* оценки разделимости представлены в табл. 4.

Таблица 4

n	r	d	Среднее значение p	Нетривиальные разложения, %
12	6	0,5	63	0
		0,84	6	0
		0,86	6	0
		0,88	6	0
		0,9	5,46	54
		0,91	5,11	89
		0,915	5,07	93
		0,92	5,005	99
		0,925	5	100
		0,93	5	100
		0,935	4,86	100
		0,94	4,63	100
		0,96	3,81	100
14	7	0,88	7	0
		0,89	7	0
		0,9	7	0
		0,91	7	0
		0,92	7	0
		0,925	6,71	29
		0,93	6,24	76
		0,935	6,03	97
		0,94	6	100
15	7	0,93	7	0
		0,935	7	0
		0,94	7	0
		0,945	6,71	29
		0,947	6,36	64
		0,95	6,04	96
		0,955	6,01	99
		0,96	6	100
16	8	0,93	8	0
		0,94	8	0
		0,95	7,05	95
		0,955	7,02	98
		0,96	7	100

Анализируя результаты эксперимента 1, можно заметить, что разделимость функции находится в непосредственной зависимости от степени неопределенности функции. Чем больше степень неопределенности d, тем больше вероятность, что для этой функции удастся построить нетривиальное разложение и уменьшить число аргументов функций g, h_i, входящих в разложение (1) в сравнении с числом n аргументов декомпозируемой функции. С ростом числа переменных возрастает вероятность разделения случайной частичной булевой функции при разбиении множества аргументов «пополам»: так,

для функций от 14 переменных можно наверняка получить нетривиальные разложения для частичных функций с 94% неопределенных значений, для функций от 16 переменных – уже для функций с 96% неопределенных значений. Зависимость доли R функций, имеющих нетривиальные разложения, от степени неопределенности d функций показана на рис. 2–4. На рис. 2 видно, что случайная функция, зависящая от 12 аргументов, степень неопределенности d которой не превышает 0,88, будет неразделима или разделима, если степень неопределенности будет больше 0,92, для случая перекодирования шести аргументов. Аналогичные скачкообразные переходы от свойства «неразделимость» к свойству «разделимость» при увеличении степени неопределенности для $n = 14$, $r = 7$ и для $n = 15$, $r = 7$ показаны на рис. 3 и 4 соответственно. Для значений параметров $n = 12$, $r = 6$ на рис. 5 показано уменьшение числа p промежуточных функций в разложении (1) при увеличении степени неопределенности d. Аналогичный график представлен на рис. 6 для $n = 16$, $r = 8$.

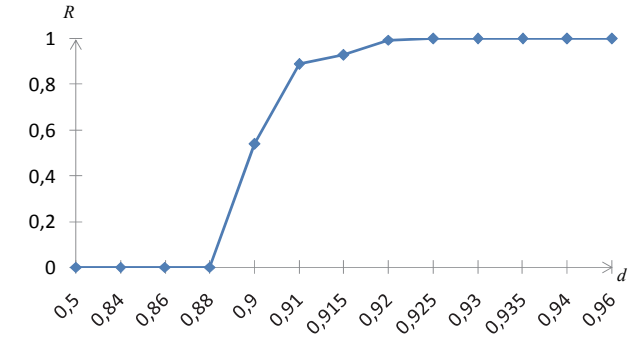

Рис. 2. Увеличение доли R разделимых функций при увеличении степени неопределенности d; фиксированные параметры $n = 12$, $r = 6$

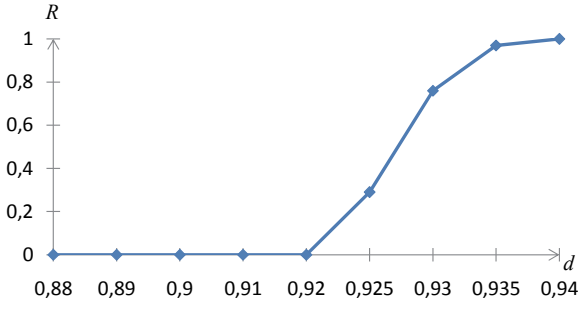

Рис. 3. Увеличение доли R разделимых функций при увеличении степени неопределенности d; фиксированные параметры $n = 14$, $r = 7$

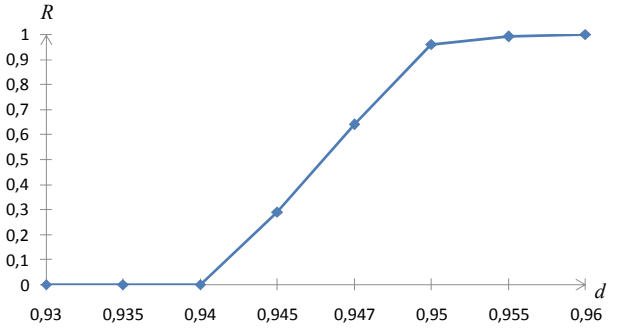

Рис. 4. Увеличение доли R разделимых функций при увеличении степени неопределенности d; фиксированные параметры $n = 15$, $r = 7$

Для ***точного алгоритма*** оценки разделимости результаты эксперимента 1 представлены в табл. 5, 6. Аналогичные «скачки» перехода к свойству разделимости наблюдаются и в данном случае, когда ищется минимальное число промежуточных функций.

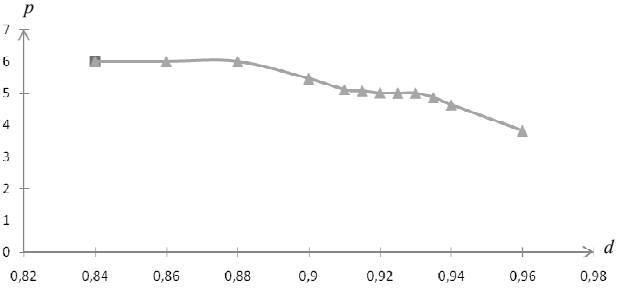

Рис. 5. Зависимость числа p промежуточных функций h от d – степени неопределенности функции; фиксированные параметры $n = 12$, $r = 6$

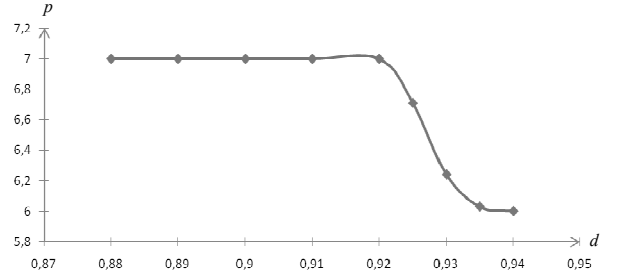

Рис. 6. Зависимость числа p промежуточных функций h от d – степени неопределенности функции; фиксированные параметры $n = 16$, $r = 8$

Поясним результаты эксперимента 1, приведенные в табл. 5, 6. Рассмотрим строку в табл. 5, выделенную жирным шрифтом: в данном случае декомпозируется 100 частичных функций от шести переменных ($n = 6$) по случайно выбранным подмножествам Y, состоящим из трех переменных, степень неопределенности всех таких функций равна 0,6 (функции заданы на 16 наборах).

Таблица 5

n	r	d	Число функций	$p=0$	$p=1$	$p=2$	$p=3$
		0	100				100\100
		0,1	100				100\100
		0,2	100		0\100	0\100	100\100
		0,3	100		0\100	1\100	100\100
		0,4	100		0\100	11\100	100\100
		0,5	100		0\100	53\100	100\100
6	**3**	**0,6**	**100**		**0\100**	**93\100**	**85\85**
		0,7	200		0\200	194\194	75\75
		0,75	200	0\2	0\191	162\162	20\20
		0,8	200	0\12	0\174	92\92	3\3
		0,85	200	0\34	0\111	33\33	
		0,9	200	0\43	0\41	4\4	
		0,1	100		0\100	0\100	100\100
		0,2	100		0\100	0\100	100\100
		0,3	100		0\100	0\100	100\100
		0,4	100		0\100	0\100	100\100
		0,5	100		0\100	0\100	100\100
		0,6	100		0\100	0\100	100\100
8	4	0,7	100		0\100	1\100	100\100
		0,8	100		0\100	94\100	100\100
		0,9	100		0\98	92\92	23\23
		0,92	100		0\95	53\53	1\1
		0,94	100		0\66	15\15	
		0,96	100		0\25	3\3	
		0,98	100		0\3		
		0,1	100		0\100	0\100	100\100
		0,2	100		0\100	0\100	100\100
		0,3	100		0\100	0\100	100\100
		0,4	100		0\100	0\100	100\100
10	5	0,5	100		0\100	0\100	100\100
		0,6	100		0\100	0\100	100\100
		0,7	100		0\100	0\100	100\100
		0,8	100		0\100	0\100	100\100
		0,9	100		0\100	99\100	100\100

В столбце $p=1$ приводится значение 0\100 – это означает, что нет ни одной функции (из испытанных 100), для которой существует разделение (1) с одной ($p=1$) промежуточной функцией. В столбце $p=2$ приводится значение 93\100 – это означает, что 93 функции (из испытанных 100 функций) имеют представление (1) с двумя ($p=2$) промежуточными функциями. В столбце $p=3$ приводится значение 85\85 – это означает, что все 85 функций (из испытанных 85 функций) имеют разделение (1) с тремя ($p=3$) промежуточными функциями.

В общем случае запись $\alpha\backslash\beta$ для столбца $p=\gamma$ в табл. 5 и 6 означает, что испытано β функций и α из них имеют γ промежуточных функций в представлении (1).

Таблица 6

n	r	d	Число функций	$p=1$	$p=2$	$p=3$
		0,1	100	0\100	0\100	100\100
		0,2	100	0\100	0\100	100\100
		0,3	100	0\100	0\100	100\100
		0,4	100	0\100	0\100	100\100
		0,5	100	0\100	0\100	100\100
12	6	0,6	100	0\100	0\100	100\100
		0,7	100	0\100	0\100	100\100
		0,8	100	0\100	0\100	100\100
		0,9	100	0\100	0\100	100\100
		0,91	100	0\100	0\100	100\100
		0,96	100	0\100	99\100	100\100
		0,1	100	0\100	0\100	100\100
		0,2	100	0\100	0\100	100\100
		0,3	100	0\100	0\100	100\100
		0,4	100	0\100	0\100	100\100
		0,5	100	0\100	0\100	100\100
14	7	0,6	100	0\100	0\100	100\100
		0,7	100	0\100	0\100	100\100
		0,8	100	0\100	0\100	100\100
		0,9	100	0\100	0\100	100\100
		0,94	25	0\25	0\25	25\25
		0,95	25	0\25	0\25	25\25
		0,97	25	0\25	18\25	25\25
		0,1	25	0\25	0\25	25\25
		0,2	25	0\25	0\25	25\25
		0,3	25	0\25	0\25	25\25
		0,4	25	0\25	0\25	25\25
16	8	0,5	25	0\25	0\25	25\25
		0,6	25	0\25	0\25	25\25
		0,7	25	0\25	0\25	25\25
		0,8	25	0\25	0\25	25\25
		0,9	25	0\25	0\25	25\25

Эксперимент 2. Как влияет мощность множества Y на разделимость функции ?

Для каждого значения параметров $n=14$, $d=0{,}97$, $s^1=s^0$ генерировалось 15 псевдослучайных булевых функций, для каждой из них случайным образом выбиралось множество Y фиксированной мощности r ($r=7, 6, 5, 4, 3, 2$) и предпринималась попытка построения разложения (1) с помощью *быстрого* алгоритма. Подсчитывалось число функций, для которых существовало нетривиальное разложение. Результаты эксперимента 2, представленные в табл. 7, показывают, что для получения нетривиальных разложений целесообразно проводить разбиение множества X на равномощные подмножества Y, Z.

Результаты нахождения минимального значения p (с помощью *точного алгоритма*) при

изменении мощности подмножества Y представлены в табл. 8. Поясним первую строку табл. 8: 12 (из 15) функций разделимы и имеют две промежуточные функции $h_1(\underline{y})$, $h_2(\underline{y})$ в представлении (1); три (из 15) функции имеют в представлении три промежуточные функции $h_i(\underline{y})$.

Таблица 7

Мощность множества Y (r)	Число функций, имеющих нетривиальное разложение (1)
7	15
6	15
5	14
4	4
3	0
2	1

Таблица 8

Мощность r множества Y	Число функций, имеющих разложение (1)	
	$p_{\min} = 2$	$p_{\min} = 3$
7	12	3
6	11	4
5	11	4
4	11	4
3	9	6
2	15	0

Эксперимент 3. Как влияет увеличение доли единичных значений на разделимость функции ?

В данном эксперименте множества M_f^1, M_f^0 имели различную мощность, однако сумма $v_0 + v_1$ мощностей множеств M_f^1, M_f^0 оставалась неизменной, т.е. s^1, s^0 имели различные значения, однако суммарное значение $s = s^1 + s^0$ оставалось неизменным. Усреднение осуществлялось по четырем функциям с одинаковыми параметрами n = 12, r = 6, s = 0.9. Параметр s^1 увеличивался от 0,5 до 0,98, в результате наблюдалось уменьшение (использовался *быстрый алгоритм*) числа p от p =5 до p = 4. Аналогично установлено, что увеличение доли нулевых значений функции при постоянном значении S также ведет к уменьшению числа p промежуточных функций.

Использование *точного алгоритма* проверки разделимости на 10 функциях (n = 12, r = 6) позволило получить следующие выводы: при увеличении параметра s^1 от 0,5 до 0,89 значение $p_{\min}$ было равным трем, в диапазоне значений s^1 от 0,9 до 0,99 значение $p_{\min}$ равнялось двум. Эксперимент 3 показал, что неравномерность значений s^1, s^0 ведет к большей вероятности разделения функции.

Эксперимент 4. Как влияет число функций системы на разделимость?

Для частичных векторных функций исследовано свойство разделимости в зависимости от увеличения числа m компонент декомпозируемой векторной функции $\underline{f}(\underline{x}) = (f^1(\underline{x}), ..., f^m(\underline{x}))$. Для векторной булевой функции $\underline{f}(\underline{x})$ рассматривалась задача получения нетривиальных разложений

$$\underline{f}(\underline{x}) = \underline{f}(\underline{y}, \underline{z}) = \underline{g}(\underline{h}(\underline{y}), \underline{z}), \qquad (5)$$

где $\underline{h}(\underline{y}) = (h_1(\underline{y}), ..., h_p(\underline{y}))$.

В эксперименте 4 были зафиксированы следующие параметры: n = 12, r = 6, d = 0,985, $s^1 = s^0$. Результат эксперимента представлен на рис. 7. Эксперимент показал, что при увеличении числа m функций системы для разделимости требуется большая степень неопределенности. На рис. 8 показана зависимость времени получения логического КНФ-уравнения при увеличении числа функций в системе. Очевидно, увеличение числа функций системы ведет к увеличению времени получения логического уравнения, а именно это время занимает основную долю времени декомпозиции, так как *SAT*-программы решают получаемые КНФ-уравнения очень быстро. Например, для n = 12, r = 6, d = 0,9 время построения графа G составляет 1,680 с, а время решения логического уравнения – 0,070 с, т.е. в 24 раза меньше. Для *SAT*-программ, решающих получаемые логические уравнения, большее значение имеет число переменных в логическом уравнении в сравнении с числом дизъюнктов в уравнениях. Это подтверждается тем, что при уменьшении степени неопределенности время решения уравнения растет незначительно, хотя число дизъюнктов в этих случаях значительно увеличивается.

Были проведены эксперименты с примерами систем функций, возникающими в практике промышленного проектирования. Системы функций были заданы на 1000 наборах и характери-

зовались следующим набором параметров: $n = 17$, $r = 9$, $m = 60$. Для таких примеров векторных функций получение логического уравнения и его решение происходит за практически приемлемое время.

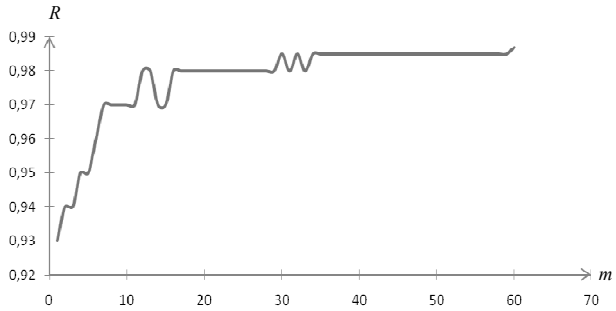

Рис. 7. Увеличение доли R нетривиально разделимых систем функций при увеличении числа m функций системы; фиксированные параметры $n = 12$, $r = 6$, $d = 0{,}985$

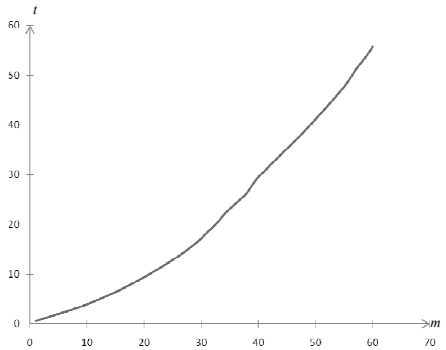

Рис. 8. Зависимость времени декомпозиции от числа m функций в системе

Заключение. Для случайных булевых функций характерен скачкообразный (в узких границах) переход от неразделимости к разделимости при увеличении степени неопределенности. Для получения нетривиальных разложений декомпозицию лучше проводить по разбиению множества аргументов X декомпозируемой частичной функции на равномощные блоки Y, Z. Эксперименты показали, что при увеличении числа аргументов декомпозируемых функций и увеличении степени неопределенности, число p промежуточных функций уменьшается. Основное время для проверки разделимости функции занимает составление логического уравнения, известные *SAT*-программы решают полученные КНФ-уравнения чрезвычайно быстро. Результаты экспериментов дополняют и уточняют известные [2] экспери ментальные результаты по проверке декомпозиционных свойств псевдослучайных булевых функций и систем, а также показывают практическую возможность применения эффективных программ решения задачи о выполнимости КНФ не только для верификации, но и для синтеза логических схем, осуществляемого методами функционального разделения.

1. *Sasao T.* FPGA design by generalized functional decomposition // Representations of discrete functions. – Kluwer Academic Publishers, 1996. – P. 233–258.
2. *Бибило П.Н.* Декомпозиция булевых функций: обзор // Проектирование устройств логического управления. – М.: Наука, 1984. – С. 106–126.
3. *Бибило П.Н.*, *Енин С.В.* Синтез комбинационных схем методами функциональной декомпозиции. – Минск: Наука и техника, 1987. – 189 с.
4. *Поттосин Ю.В.*, *Шестаков Е.А.* Табличные методы декомпозиции систем полностью определенных булевых функций. – Минск: Беларус. навука, 2006. – 327 с.
5. *Бибило П.Н.* Декомпозиция булевых функций на основе решения логических уравнений. – Минск: Там же, 2009. – 211 с.
6. *Закревский А.Д.* Логический синтез каскадных схем. – М.: Наука, 1981. – 416 с.
7. *Брейтон Р.К.*, *Хэчтел Г.Д.*, *Санджованни-Винчентелли А.Л.* Синтез многоуровневых комбинационных логических схем // ТИИЭР. – 1990. – Т. 78. – № 2. – С. 38 – 83.
8. *Каммозев Н.Ф.*, *Сычев А.Н.* Спектральный метод декомпозиции булевых функций // Автоматика и вычислительная техника. – 1979. – № 2. – С. 54–58.
9. *Lee R.-R.*, *Jiang J.-H.R.*, *Hung W.-L.* Bi-decomposing large Boolean functions via interpolation and satisfiability solving // Design Automation: proceedings of the 45th annual conf., Anaheim, California, 8–13 Jun. 2008. – NY: ACM, 2008. – P. 636–641.
10. *Kunz W.*, *Marques-Silva J.*, *Malik S.* SAT and ATPG: Algorithms for Boolean Decision Problems // Logic synthesis and verification. – Kluwer Academic Publishers, 2002. – P. 309 – 341.
11. *http*://satcompetition.org
12. *Goldberg E.*, *Novikov Y.* BerkMin: a Fast and Robust Sat-Solver // Proc. of Design, Automation and Test in Europe (DATE02), 4–8 March, 2002. – P. 142–149.

Поступила 19.09.2011
Тел. для справок: +375 (17) 284-2084 (Минск)
E-mail: *bibilo@newman.bas-net.by*