УДК 618.5.004

Ю. А. Кочкарев, д-р техн. наук, **С. А. Кущ**
Черкасский государственный технологический университет
(Украина, 18006, Черкассы, бульв. Шевченко, 460,
тел. (0472) 730217, E-mail: kushch09@rambler.ru)

Представление и реализация логических функций в родственной форме

Поставлена и проанализирована задача реализации булевых логических функций в родственной форме (Р-форме). Приведены практические примеры целесообразности и необходимости использования Р-формы и сформированы типичные этапы ее получения и минимизации для заданной логической функции.

Поставлено і проаналізовано задачу реалізації булевих логічних функцій у спорідненій формі (С-формі). Наведено практичні приклади доцільності та необхідності використання С-форми та сформовано типові етапи її отримання та мінімізації для заданої логічної функції.

К л ю ч е в ы е с л о в а: Р-*форма, форма представления, логическая функция, доопределение функций.*

Классическая задача проектирования цифровых автоматов (ЦА) заключается в минимальной реализации соответствующих комбинационных схем (КС), которые являются информационным ядром ЦА. Комбинационные схемы в ЦА реализуют системы логических функций (ЛФ), состоящие из m ЛФ от n аргументов [1]. Одним из этапов задачи реализации КС является минимизация ЛФ, которые входят в систему и, как правило, заданы в виде таблицы истинности (ТИ).

Интенсивное расширение множества функций, выполняемых ЦА в информационных технологиях, приводит к неминуемому пересмотру рамок классической задачи проектирования ЦА. Проанализируем ситуации, когда переход от ТИ к схеме или алгоритму функционирования ЦА становится неоднозначным и, несмотря на это, остается эффективным с практической точки зрения, т.е. рассмотрим типичные случаи, когда реализация ЦА выходит за указанные рамки классической задачи.

1. Развитие информационной интеграции зависит от эффективности защиты информации, в основе которой лежат криптографические механизмы. В настоящее время широко применяются специальные булевы функции, так называемые криптографические функции (КФ), которые в

наибольшей степени обеспечивают стойкость к влиянию криптоанализа [2]. Построение КФ обычно происходит в два этапа: построение ЛФ для части строк ТИ с учетом условий, накладываемых криптографическим преобразованием, и доопределение функций на остальных строках согласно условиям сохранения так называемых SAC-свойств (Strict Avalance Criterion) ЛФ, т.е. обеспечение максимума полной и условной энтропии, соответствующее максимуму устойчивости против криптоанализа [2].

Следует заметить, что в данном случае на этапе реализации ЛФ допускается некоторое множество допустимых решений, причем их допустимость определяется уровнем «близости» элементов этого множества к некоторому оптимуму, который на этапе проектирования может быть априорно неизвестным.

2. Реальные КС, как и любые устройства, не застрахованы от сбоев, т.е. от временных (спорадических) или постоянных отклонений выходов сигналов КС от заданных по ТИ значений. В зависимости от конкретных условий работы КС каждый такой сбой может привести к следующему:

- невозможности дальнейшей работы КС;
- самообновлению работы КС после самоликвидации причины сбоя;
- компенсированию выходов КС с помощью дополнительных специальных блоков контроля и коррекции (если они есть);
- ситуации, когда сбой КС остался незамеченным, так как не привел к ощутимым последствиям.

Наибольший интерес представляют два последних случая. Специальные блоки контроля и коррекции, которые иногда включаются на выходе КС, применяются в системах, склонных по своей природе к влиянию помех, например в линиях связи, криптографических блоках, системах стеганографии и др. В рассматриваемой ситуации для реализации ЦА также допускается некоторое множество приемлемых решений, и приемлемость их определяется уровнем близости, т.е. точностью реализации оператора преобразования информации в цифровом блоке (ЦБ) с учетом коррекции.

3. Незамеченными сбои в ЦБ могут быть в случаях, когда сигнал на выходе КС близок по достоверности к точному значению. Такая ситуация может возникнуть, например, если ЦБ обрабатывает аналоговый сигнал после аналогоцифрового преобразования (АЦП). При этом ошибка в одном или даже в нескольких младших разрядах на выходе АЦП, и соответственно, на выходе КС, — несущественна и поэтому может остаться незамеченной.

Для описанных случаев общим является тот факт, что при реализации КС в качестве приемлемого результата возможно не одно, а несколько

допустимых решений. Следовательно, будем рассматривать ситуацию, когда классическая задача реализации КС, т.е. системы логических уравнений, состоящей из m заданных ЛФ, преобразуется к задаче реализации системы функций

$$Z_1 = f_1[X^{(n)}] \vee F_{11}[X^{(n)}] \vee ... \vee F_{1p_1}[X^{(n)}];$$
$$Z_m = f_m[X^{(n)}] \vee F_{m1}[X^{(n)}] \vee ... \vee F_{mp_m}[X^{(n)}], \quad (1)$$

где $X^{(n)}$ — вектор аргументов размерности n, т.е. вектор дискретных сигналов на входах КС; $f_1[X^{(n)}]$, ..., $f_m[X^{(n)}]$ — ЛФ, задаваемые для КС с помощью ТИ или другим способом, т.е. реализующие номинальный режим работы КС; $F_{11}[X^{(n)}]$, ..., $F_{1p_1}[X^{(n)}]$— допустимые варианты реализации точной функции $f_1[X^{(n)}]$; $F_{m1}[X^{(n)}]$, ..., $F_{mp_1}[X^{(n)}]$— допустимые варианты реализации точной функции $f_m[X^{(n)}]$.

Далее будем опускать указания на очевидную зависимость от $X^{(n)}$ всех компонентов (1), и систему (1) запишем в виде

$$Z_1 = f_1 \vee F_{11} \vee ... \vee F_{1p_1};$$
$$Z_m = f_m \vee F_{m1} \vee ... \vee F_{mp_m}. \quad (2)$$

Из (2) видно, что в предложенной системе каждая ЛФ из m заданных в виде ТИ или другим способом в общем случае может быть реализована в виде ρ_i родственных (близких) вариантов.

Таким образом, система (2) представляется обобщением классической постановки задачи реализации КС. В частности, заметим, что классическая постановка указанной задачи вписывается в (2) как частный случай, когда для всех ρ_i в системе (2) $\rho_i = 1$.

Введем необходимые определения. Реализацию КС, в которой каждая исходная ЛФ Z_i может быть представлена в виде некоторого числа вариантов, назовем родственной реализацией. Исходные ЛФ Z_i, выбранные для окончательной реализации КС, т.е. как оптимальные из ρ_i вариантов по некоторому критерию, назовем родственной ЛФ (РЛФ), а выбранную из ρ_i вариантов форму представления (ФП) для РЛФ назовем родственной ФП (РФП).

Таким образом, введем новую форму реализации КС и новую форму представления ЛФ — РФП. При этом заметим, что любая КС может быть реализована в Р-форме (все $\rho_i = 1$). Следует заметить также, что любая ЛФ F_{ik} из (2) должна быть достаточно близкой к номинальной f_i, причем в четко определенном для каждой ситуации значении, так как в противном случае система (2) становится неопределенной. Кроме того, близость F_{ik} и f_i может быть оценена различными способами в зависимости от условий работы КС и ЦА в целом.

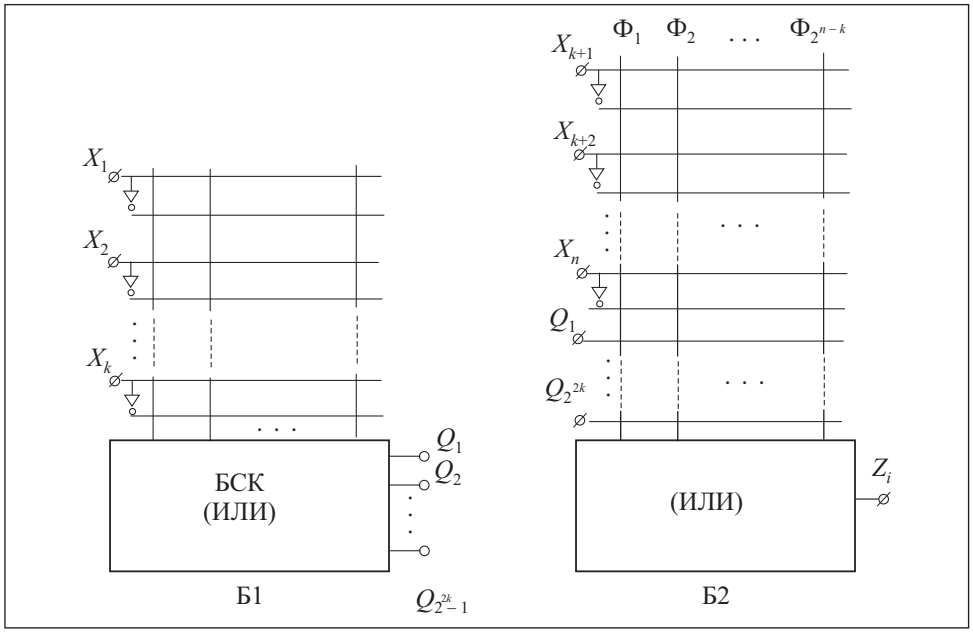

Рис. 1. Схема реализации ЛФ в РФП

Теперь рассмотрим систему уравнений (2) с формальной точки зрения. Каждая ЛФ из (2) может быть представлена в виде обобщенного ряда:

$$Z_i(x_1, x_2, ..., x_n) = \sum_{i=0}^{2^n-1} Q_{ij}(x_k)\,\Phi_{ij}(x_{n-k}), \qquad (3)$$

где Q_{ij} — так называемые информативные функции [1], являющиеся весовыми коэффициентами ряда (3) и зависящие от числа компонентов вектора аргументов x_k $(0 \le k \le n)$; $\Phi_{ij}(x_{n-k})$ — базисные функции, являющиеся ортами системы координат при разложении ЛФ в ряд; знак Σ обобщенного суммирования членов ряда (3) может принимать значение дизъюнкции в классической ФП (КФП), алгебраического суммирования в алгебраической ФП (АФП) или суммирования по mod2 в Рида—Мюллера ФП (РМФП) [3].

На рис. 1 приведена типовая схема Р-реализации КС, состоящая из двух блоков — Б1, в котором формируются информативные функции Q_i, и Б2, в котором формируются базисные функции Φ_i, а также заданная ЛФ Z_i. Число входных шин в Б1 составляет $2k$, если формирование Q_i выполняется в КФП, или в два раза меньше и без входных инверторов, если применяется АФП или РМФП. Блок суммирования конъюнкций (БСК) в Б1 должен соответствовать

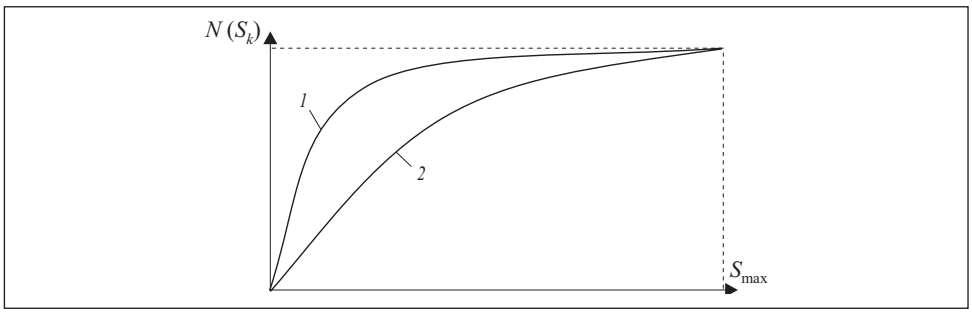

Рис. 2. Зависимость $N(S_k)$: *1* — более совершенная ФП; *2* — менее совершенная ФП

выбранной ФП для Q_i. Для КФП блок суммирования — это линейка с функциями ИЛИ.

Число базисных функций Φ_i в Б2 составляет 2^{n-k}, где k — число аргументов x_i, выделенных для Q_i. Шины Φ_i после логического доумножения на Q_i подключены к выходной линейке функций ИЛИ, на которой окончательно формируется заданая ЛФ Z_i.

Для реализации новой формы РФП и введения ее в широкую инженерную практику требуется решение следующих задач:

$З_0$. Исследование объективной конкурентоспособности РФП по сравнению с известными ФП ЛФ (КФП, АФП, РМФП), а также с новыми ФП ЛФ, которые будут появляться.

$З_1$. Формирование базы данных вариантов оценки близости точных ЛФ f_i из системы (2) и приближенных к ним F_{ip_1}.

$З_2$. Разработка методов минимизации ЛФ в РФП и схемотехники родственной реализации КС в случае подтверждения конкурентоспособности РФП.

$З_3$. Разработка подходов к сравнению вариантов F_{ip_1} в (2), т.е. решение оптимизационной задачи формирования РЛФ.

Рассмотрим задачи $З_0$—$З_3$. Для объективного определения перспективности РФП целесообразно использовать технологию, примененную в [3] для сравнения трех известных на тот момент базисных ФП — КФП, АФП и РМФП — на полных множествах ЛФ $L(n)$ ($n \le 4$). Позднее такое же сравнение было проведено для $L(n)$ при $n = 5$. Технология сравнения эффективности различных ФП заключается в том, что для каждой ФП определяется так называемая функция сложности реализации, т.е. зависимость числа ЛФ $N(S_k)$, которые можно реализовать, от заданного показателя сложности S_k.

На рис. 2 показана зависимость $N(S_k)$ для любой ФП и любого критерия оценки сложности S_k. При $S = 0$ $N(S) = 0$, а максимальное значение

$N(S)$ равняется 2^{2^n}. Площадь криволинейной трапеции $N(S)$, отнесенная к площади прямоугольника $[2^{2^n}, S_{\max}]$, может быть применена для сравнения значения эффективности ФП в избранном показателе сложности S_k.

В таблице приведены мощности подмножеств приоритетов по наиболее важному показателю S_s — площади микросхемы в условных единицах. Этот показатель необходим для реализации заданных ЛФ на полных множествах $L(n)$.

Следует заметить, что нижнюю оценку эффективности РФП можно определить без каких-либо вычислений. Она должна равняться эффективности КФП, так как КФП является составной частью РФП. Из таблицы видно, что конкурентоспособность РФП выше по сравнению, например, с КФП, наиболее распространенной в настоящее время. При разработке более эффективных методов минимизации (задача $З_2$) число ЛФ с оптимальной РФП, безусловно, будет увеличиваться.

Формирование вариантов оценки близости между точными ЛФ f_i и РЛФ в системе (2) нуждается в специальных исследованиях. Однако для случаев 1 и 2 можно предложить следующие варианты формирования:

• для реализации КФ в качестве F_i могут быть приняты функции, построенные посредством доопределения частично определенных ЛФ, которые, в свою очередь, построены исходя из условий криптографических преобразований. Для каждого шага доопределения (для некоторого x_i) строится одна или несколько SAC-функций;

• при совместном использовании КС с блоками корректирования сбоев близость определяется возможностями блока корректирования: если указанный блок имеет возможность, например, корректировать сбои в одном разряде на выходе КС, то все F_i, имеющие единичное расстояние по Хеммингу, будут близкими к точному выходу КС;

• при использовании КС совместно с входным АЦП близкие функции могут быть построены посредством доопределения входов младших разрядов КС исключительно исходя из соображений простоты реализации.

Следует заметить, что множество близких функций можно дополнительно оптимизировать в случае получения одинаковых по сложности

Число аргументов	Число ЛФ в оптимальных ФП (по критерию S_s)			
	КФП	АФП	РМФП	РФП
2	0	0	2	0
3	0	48	64	6
4	0	20 296	24 494	274
5	511	5 500	44 594	7 543

реализаций F_{ip_i}, близких к f_i ЛФ. Например, для реализации КФ таким дополнительным критерием может быть максимум полной энтропии среди близких функций с одинаковой сложностью реализации.

Для КС, имеющих m выходов ($m > 1$), дополнительный практический интерес вызывает возможность совместной реализации всех ЛФ в КС, т.е. поиск одинаковых фрагментов в Q_i и в Φ_i как для различных f_i, входящих в систему (2), так и внутри каждой отдельной ЛФ в (2). Наличие одинаковых фрагментов позволяет упростить реализацию КС, что следует из рис. 1.

Решение оптимизационной задачи $З_3$ формирования РЛФ основано на том, что среди имеющихся в наличии вариантов есть наилучший, т.е. оптимальный вариант по некоторому критерию (по одному или нескольким). В качестве такого критерия в данном случае целесообразно принять минимальную сложность реализации КС. Эта задача тесно связана с задачей $З_2$, которая требует решения широкого круга проблем по прикладной теории цифровых автоматов и схемотехнике.

Выводы

Для введения в широкую инженерную практику многовариантной реализации КС необходимо следующее:

- формирование банка типичных ситуаций проектирования КС, когда родственная реализация может давать реальный эффект уменьшения показателей сложности реализации ЛФ;
- формирование банка возможных вариантов близости между точными и приемлемыми ЛФ в Р-множестве;
- разработка методов минимизации РЛФ с учетом того, что среди большого числа вариантов реализации множество классических методов являются только частными случаями ($k = 0$).

Перечень необходимых исследований неизбежно будет расширяться в ходе работы с Р-формой реализации ЛФ КС, которые являются информационными ядрами ЦА в современных системах автоматики, вычислительной техники и других элементах ИТ технологий.

This work presents and analyses for the first time the realization of the problem of Bulean logic functions in the so-called Cognate-form. The resulted practical examples show the expediency and even the necessity of the Cognate-form. Typical stages of obtaining the Cognate-form for the set logic function and its minimization were also generated.

1. *Кочкарев Ю. А.* Теория, техническая реализация и использование ортогонального уплотнения информации в вычислительных устройствах: Дис. ... д-ра техн. наук. — Таганрог, 1983.—317 с.

2. *Столлингс В.* Криптография и защита сетей. Изд 2-е. — СПб: Изд. дом «Питер», 2000.— 665 с.
3. *Кочкарев Ю. А., Казаринова Н. Л., Пантелеева Н. Н., Шакун С. А.* Классические и альтернативные минимальные формы логических функций. Каталог-справочник. — Черкассы: Ин-т управления бизнесом, 1999.—195 с.

Поступила 08.04.11

КОЧКАРЕВ Юрий Александрович, д-р техн. наук, профессор кафедры информатики и информационной безопасности Черкасского государственного технологического университета. В 1959 г. окончил Киевский политехнический ин-т. Область научных исследований — усовершенствование структуры цифровых узлов и блоков на основе альтернативных форм представления логичных функций; технические и программные способы защиты материальной и интеллектуальной собственности юридических и физических лиц.

КУЩ Сергей Александрович, ассистент кафедры информатики и информационной безопасности Черкасского государственного технологического университета, который окончил в 2008 г. Область научных исследований — разработка цифровых блоков и улучшение их параметров с помощью альтернативных форм представления логических функций.