и 1. Так как при разложении по $\vee$ уменьшается параметр $m_f^1$, а при разложении по $\wedge$ – $m_f^0$, то для выбора базисной операции на каждом шаге алгоритма можно использовать следующее эвристическое соображение: если $m_f^0 > m_f^1$, то выбираем операцию $\wedge$, иначе – $\vee$. Если для очередной компоненты разложения не находится реализующей ее функции в $\Phi$, то она, в свою очередь, подвергается разложению, и так до определения всех компонент. Процесс сходится, если выполнено условие теоремы 2.

Данный алгоритм строит однокаскадные схемы, а значит, решение в классе КМОП-схем существует, только если задана отрицательная функция либо на входы схемы вместе с каждым входным сигналом подается и его инверсия. В дальнейшем предполагается рассмотреть вопрос о выделении каскадов, преследующем двоякую цель: во-первых, расширение класса реализуемых функций и, во-вторых, упрощение получаемых схем (особенно при задании на синтез системы функций).

ЛИТЕРАТУРА


1. *Агибалов Г.П.* Дискретные автоматы на полурешетках. Томск: Изд-во Том. ун-та, 1993. 227 с.
2. *Шеннон К.* Работы по теории информации и кибернетике. М.: ИЛ, 1963. 827 с.
3. *Поваров Г.Н.* Метод синтеза вычислительных и управляющих контактных схем // Автоматика и телемеханика. 1957. № 2. С. 145–162.
4. *Агибалов Г.П., Бузанов В.А., Липский В.Б., Румянцев Б.Ф.* Логическое проектирование переключательных автоматов. Томск: Изд-во Том. ун-та, 1983. 156 с.
5. *Павлов В.Л.* О синтезе логических схем из элементов «ИЛИ–НЕ» с ограниченным числом входов // Вычислительная техника. Каунас: Каунасский политехнический институт, 1971. Т. 2. С. 219–223.



Статья представлена кафедрой защиты информации и криптографии факультета прикладной математики и кибернетики Томского государственного университета, поступила в научную редакцию 1 марта 2000 г.



УДК 519.7



*Н.Г. Парватов*


# К СИНТЕЗУ ФОРМУЛ, РЕАЛИЗУЮЩИХ И ПРЕДСТАВЛЯЮЩИХ КВАЗИМОНОТОННЫЕ И МОНОТОННЫЕ ФУНКЦИИ НА ПОЛУРЕШЕТКЕ ПОДМНОЖЕСТВ КОНЕЧНОГО МНОЖЕСТВА


Работа выполнена при финансовой поддержке РФФИ, грант № 98–01–00288



Предлагаются методы синтеза формул из одноместных функций и двухместной дизъюнкции (конъюнкции) для реализации и представления квазимонотонных и монотонных функций на полурешетке подмножеств $k$-элементного множества.


## Постановка задачи

Будем рассматривать функции, которые вместе со своими аргументами принимают значения из верхней полурешетки $C$ всех непустых подмножеств множества $E=\{0,\ldots, k-1\}$. Множество всех таких функций обозначим $P_C$. Функции из $P_C$ заслуживают внимания в связи с тем, что с их помощью удается адекватно и с наперед заданной точностью моделировать динамическое поведение интегральных схем логического управления [1]. Область определения $D_f$ любой такой функции $f$ от $n$ переменных является полурешеткой $C^n$ – $n$-й декартовой степенью полурешетки $C$. В ней элементы суть наборы длины $n$ с компонентами в $C$, отношение порядка $\leq$ есть покомпонентное включение и сложение есть покомпонентное объединение.

Функция $f$ называется *аддитивной*, если она является гомоморфизмом полурешеток, т.е. если $f(a+b)=f(a)+f(b)$ для любых $a$ и $b$ из $D_f$. Функция $f$ называется *точечной*, если ее значение на любом элементе $d$ из $D_f$ равно сумме (объединению) элементов, содержащихся в $d$. Функция $f$ называется *монотонной*, если для произвольных $a$ и $b$ из $D_f$ всякий раз из $a\leq b$ следует $f(a)\leq f(b)$. Функция $f$ *реализуется* функцией $g$, или $g$ является *реализацией* $f$, если $g(d)\leq f(d)$ при любом $d$ из $D_f$. Функция $f$ называется *квазимонотонной*, если она реализуется некоторой монотонной функцией. Множества всех аддитивных, точечных, монотонных и квазимонотонных функций в $P_C$ обозначаются соответственно $H$, $P$, $M$ и $Q$. Вместе с отношением реализации они являются частично упорядоченными множествами, причем $H$ и $P$ – собственными подмножествами в $M$, $M$ – собственным подмножеством в $Q$, $Q$ – собственным подмножеством в $P_C$, поэтому можно говорить о минимальных элементах в них. Минимальными в $Q$ функциями являются *минимальные точечные функции*, множество которых обозначается $T$. Множества всех минимальных элементов частично упорядоченного множества $S$ обозначается $m(S)$. В частности, $m(P)=m(Q)=m(M)=T$, $m(C)=E$ – множества минимальных точечных функций и одноэлементных подмножеств соответственно. Элементы в $C$ будем рассматривать и как функции в $P_C$, принимающие значения соответствующих констант и, следовательно, являющиеся точечными функциями, т.е. $C\subseteq P$, причем $m(C)\subseteq m(P)$. Введенные выше определения взяты нами из [2].

Пусть $B\subseteq Q$. Определим понятие *формулы над B* и *функции данной формулы*. Сделаем это в форме следующего индуктивного определения:

1. Пусть $x$ – символ переменной, принимающей значения в полурешетке $C$. Тогда $x$ – формула над $B$ и одноместная функция, значения которой совпадают со значениями своего аргумента – функция данной формулы.

2. Пусть $F_1,\ldots, F_m$ – формулы над $B$ и функции $f_1,\ldots, f_m$ являются функциями соответствующих формул $F_1,\ldots, F_m$. Пусть $f$ – символ $m$-местной функции из $B$. Тогда $f(F_1,\ldots, F_m)$ – формула над $B$ и $f(f_1,\ldots, \ldots, f_m)$ – функция данной формулы.

3. Других формул над $B$ нет.

Будем говорить:

– функция $f$ *реализуется формулой* $F$ или формула $F$ является *r-формулой* функции $f$, если $f$ реализуется функцией формулы $F$;

– формула $F$ является *представлением* функции $f$ или формула $F$ является *s-формулой* функции $f$, если $f$ является функцией формулы $F$.

Пусть $N$ – некоторый класс функций из $Q$ и $B \subseteq N$. Будем говорить, что система функций $B$ обладает свойством *r-полноты* (*s-полноты*) в $N$ или $B$ является *r-базисом* (*s-базисом*) в $N$, если для любой функции из $N$ существует $r$-формула ($s$-формула) над $B$.

Задача синтеза $r$- и $s$-формул для функций из $N$ в базисе $B$ ставится следующим образом: требуется указать метод, при помощи которого для любой функции из $N$ можно построить $r$- и $s$-формулу над $B$. Заметим, что задача синтеза формул для квазимонотонных функций осложняется тем, что необходимые и достаточные условия $r$-полноты, так же как и условия $s$-полноты, до сих пор неизвестны [2–4].

Договоримся не различать одноэлементные подмножества некоторого множества от соответствующих элементов данного множества: т.е. для любого множества $D$ и для любого $d$ из $D$ будем считать $d=\{d\}$.

Пусть через $x \vee y$ и $x \& y$ обозначаются минимальные точечные функции, дизъюнкция и конъюнкция, которые при $x$ из $E$ и $y$ из $E$ равны соответственно $\max(x, y)$ и $\min(x, y)$.

В настоящей работе рассматриваются методы синтеза $r$- и $s$-формул для функций из $M$ и $Q$ в монотонных и квазимонотонных базисах типа $\{\vee\} \cup B$, состоящих из функции $\vee$ и некоторого множества $B$ одноместных квазимонотонных функций, содержащего в себе множество $T^{(1)}$ всех одноместных минимальных точечных функций. Заметим, что решив задачу синтеза $r$- и $s$-формул для функций из $M$ и $Q$ в данных базисах, мы тем самым показали $r$- и $s$-полноту данных базисов в множествах $M$ и $Q$ соответственно.

Поясним постановку задачи. Данная постановка возникает в связи с проблемой синтеза комбинационных схем с заданным динамическим поведением. Если при создании обычной комбинационной схемы, функционирующей в статическом режиме, требуют, чтобы она выдавала определенные выходные сигналы при определенных комбинациях входных сигналов, то при создании комбинационных схем, функционирующих в динамическом режиме, требуется также, чтобы выходные сигналы схемы не выходили за границы заданных подмножеств при изменении входных сигналов в рамках заданных подмножеств. Оказывается, что только квазимонотонные функции физически реализуемы (допускают схемную реализацию в физически исполнимом базисе): функции реальных элементов аддитивные и точечные, функции схем из таких элементов монотонные, а функции, реализуемые схемами, квазимонотонные [1]. Так как существует взаимно однозначное соответствие между формулами в монотонных базисах и структурами комбинационных схем, то сформулированные выше задачи синтеза эквивалентны задачам синтеза комбинационных схем с определенным динамическим поведением. Поясним выбор базисных функций. Для начала заметим, что поскольку конъюнкция выражается через дизъюнкцию при помощи некоторой перестановки $s$ из $T^{(1)}$ в форме $x \& y = s^{-1}(s(x) \vee s(y))$, то описанные ниже методы синтеза в базисах типа $\{\vee\} \cup B$ легко могут быть переформулированы для базисов типа $\{\&\} \cup B$. Выбор же функций $\&$ и $\vee$ в качестве базисных не случаен. Дело в том, что для большого класса комбинационных схем, а именно для тех комбинационных схем, в которых элементами из множества $E$ моделируются проводимости цепей, функции $\&$ и $\vee$ моделируют соответственно последовательное и параллельное соединения проводников и, следовательно, содержатся в любом реальном базисе. В этом случае приводимые в данной работе методы позволяют создавать плоские схемы из функциональных элементов, соответству-ющих функциям из $T^{(1)}$. Функции же из $T^{(1)}$ являются в некотором смысле простейшими в $Q$, и на синтез схем для них могут быть естественным образом распространены известные методы синтеза схем для одноместных функций $k$-значной логики.

## Синтез $r$-формул для квазимонотонных функций в базисе $\{\vee\} \cup T^{(1)}$

Введем необходимые обозначения.

Для произвольной функции $f$ в $Q$ и для произвольного элемента $c$ в $C$ пусть $V_f = f(D_f) = \{f(d): d \in D_f\}$. $M_f^c = \{d \in D_f : f(d) \cap c = \varnothing\}$, $D_f^c = \{d \in D_f : f(d) = c\}$ и $\max(M_f^c)$ есть множество максимальных элементов в $M_f^c$.

Введем в рассмотрение специальный класс квазимонотонных функций $\Phi$, определив его при помощи выражения: $\Phi = \{f \in Q : \forall c \in C(|M_f^c| \le 1)\}$.

Для числа $j$ в $\{1,...,m\}$, вектора $u=(u_1,..., u_m)$ в $C^m$ и подмножества $U \subseteq C^m$ обозначим через $[u]_j$ – $j$-ю компоненту $u_j$ вектора $u$, через $[U]_j$ – множество $\{[u]_j : u \in U\}$ $j$-х компонент векторов из $U$, через $\inf(U)$ – точную нижнюю грань множества $U$ в полурешетке $C^m$ (которая есть покомпонентное пересечение элементов из $U$); причем будем считать, что $\inf(U)=\varnothing$, если таковая отсутствует.

Для произвольного множества $A$ обозначим через $A^{(m)}$ множество всех $m$-местных функций в $A$.

Будем говорить, что функция $f$ разлагается по функции $g \in Q^{(m)}$ на компоненты $f_1,...,f_m$, если $f = g(f_1,..., f_m)$.

Обозначим $S$ множество перестановок в $T^{(1)}$. Каждая функция $s$ в $S$ имеет в $S$ обратную функцию $s^{-1}$ такую, что $\forall x \in C(ss^{-1}(x) = s^{-1}s(x) = x)$.

Сформулируем сначала тест квазимонотонности из [1].

**Тест квазимонотонности.** Функция $f: C^m \to C$ квазимонотонна, если и только если для любого подмножества $U \subseteq C^m$, имеющего нижнюю грань в $C^m$, подмножество $f(U) \subseteq C$ имеет нижнюю грань в $C$.

Так как в верхней полурешетке существование нижней грани равносильно существованию точной нижней грани, то в формулировке теста вместо «нижняя грань» можно читать «точная нижняя грань», чем мы и будем пользоваться в дальнейшем без дополнительных оговорок.

Докажем необходимые утверждения.

**Лемма 1.** Пусть $f\in Q^{(m)}$ и $\forall U\subseteq C^m(\inf([U]_j)\neq\varnothing\Rightarrow \Rightarrow\inf(f(U))\neq\varnothing)$. Тогда $\exists s\in T^{(1)}(f(x_1,..., x_m)\geq s(x_j))$.

Доказательство. Для произвольного элемента $c$ в $C$ положим $D_c=\{d\in C^m:[d]_j\geq c\}$. Построим одноместную функцию $p$ для произвольного $c$ из $C$, положив $p(c)=\inf(f(D_c))$. Так как по построению $\inf([D_c]_j)=c$, то $\inf(f(D_c))\neq\varnothing$, и данное определение функции корректно. Заметим, что $f(x_1,..., x_m)\geq p(x_j)$.

Покажем квазимонотонность функции $p$. Пусть $U\subseteq C$, $U=\{u_1,..., u_r\}$ и $u=\inf(U)\neq\varnothing$. Тогда $p(U)=\{p(u_1),..., p(u_r)\}=\{\inf(f(D_{u1})),...,\inf(f(D_{ur}))\}$, $\inf(p(U))=\inf\{f(D_{u1}),..., f(D_{ur})\}=\inf(f(D_{u1}\cup...\cup D_{ur}))$. Так как $\inf([D_{u1}\cup...\cup D_{ur}]_j)=[u]_j\neq\varnothing$, то, по условию леммы $\inf(f(D_{u1}\cup ...\cup D_{ur}))\neq\varnothing$ и, следовательно, $\inf(p(U))\neq\varnothing$, откуда по тесту квазимонотонности следует, что $p\in Q$. Значит, в качестве функции $s$ можно взять любую функцию из $T^{(1)}$, реализующую функцию $p$.

**Следствие.** Пусть $f\in Q^{(m)}$ и $\forall U\subseteq C^m(\inf(f(U))=\varnothing\Rightarrow\inf([U]_j)=\varnothing)$. Тогда $\exists s\in T^{(1)}(f(x_1,..., x_m)\geq s(x_j))$.

**Лемма 2.** Пусть $f\in\Phi^{(m)}$. Тогда $\exists j\in\{1,..., m\}$ $\exists s\in T^{(1)}(f(x_1,..., x_m)\geq s(x_j))$.

Доказательство. Если $\inf(V_f)\neq\varnothing$, то функция $f$ реализуется константой в $C$. Поэтому рассмотрим случай $\inf(V_f)=\varnothing$. Пусть $V=\{v\in V_f:\exists A\subseteq V_f(\inf(A)\neq\varnothing\ \&\ \inf(A\cup v)=\varnothing)\}$. Тогда $V_f-V=\{v\in V_f:\forall A\subseteq V_f(\inf(A)\neq\varnothing\Rightarrow\inf(A\cup v)\neq\varnothing)\}$. Так как $\inf(V_f)=\varnothing$, то $V\neq\varnothing$ и из определения класса $\Phi$ следует, что $\forall v\in V(|D_f^v|=1)$.

Пусть $v$ – произвольный элемент из множества $V$. Тогда $\inf(V-v)\neq\varnothing$. Покажем это. Из определения множества $V$ следует, что $\exists A\subseteq V_f(\inf(A)\neq\varnothing\ \&\ \inf(A\cup v)=\varnothing)$. Пусть $A'=A\cap V$ и $A=A'\cup\{a_1,.., a_r\}$, где $\{a_1,.., a_r\}=(V_f-V)\cap A$. Тогда $\inf(A')\neq\varnothing$, так как $\inf(A)\neq\varnothing$ и $A'\subseteq A$. Покажем, что $\inf(A'\cup v)=\varnothing$. Предположим, что $\inf(A'\cup v)\neq\varnothing$. Пользуясь определением множества $V_f-V$ и фактом $\{a_1, ..., a_r\}\subseteq V_f-V$, получим $\inf(A'\cup v)\neq\varnothing\Rightarrow\inf(A'\cup a_1\cup v)\neq\varnothing\Rightarrow \Rightarrow\inf(A'\cup a_1\cup a_2\cup v)\neq\varnothing\Rightarrow\inf(A'\cup a_1\cup a_2\cup...\cup a_r\cup v)=\inf(A\cup v)\neq \neq\varnothing$. Пришли к противоречию. Следовательно, $\inf(A'\cup v)=\varnothing$. Заметим, что $v\notin A$, $v\notin A'$. Пусть $V-v-A'=\{v_1..., v_l\}$. Из определения класса $\Phi$ следует, что $\inf(A'\cup v_1)\neq\varnothing$, откуда, в свою очередь, следует $\inf(A'\cup v_1\cup v_2)\neq\varnothing$ и т.д. Применяя индукцию, получим $\inf(A'\cup v_1\cup v_2\cup... ...\cup v_l)=\inf(V-v)\neq\varnothing$.

Предположим, что существует такое подмножество $U$ множества $V_f$, что $\inf(U)=\varnothing$ и $V$ не содержится в $U$. Пусть $U'=U\cap V$, $U=U'\cup\{u_1,..., u_l\}$. Так как $V$ не содержится в $U$, то $U'\subset V$ и $\exists v\in V((V-v)\supseteq U')$. А так как $\inf(V-v)\neq\varnothing$, то и $\inf(U')\neq\varnothing$. Из определения $V$, так как $\{u_1,...,u_l\}\subseteq V_f-V$, то $\inf(U'\cup u_1)\neq\varnothing\Rightarrow\inf(U'\cup u_1\cup u_2)\neq\varnothing\Rightarrow...\Rightarrow\inf(U'\cup u_1\cup u_2\cup... ...\cup u_l)=\inf(U)\neq\varnothing$ Полученное противоречие доказывает, что $\forall U\subseteq V_f$ $(\inf(U)=\varnothing\Rightarrow U\supseteq V)$. Так как верно $\forall U\subseteq \subseteq V_f(U\supseteq V\Rightarrow\inf(U)=\varnothing)$, то $\forall U\subseteq V_f(U\supseteq V\Leftrightarrow\inf(U)=\varnothing)$.

Пусть $D^v=\{d\in D_f:f(d)\in V\}$. Так как $\inf(f(D^v))=\inf(V)\neq\varnothing$, то по тесту квазимонотонности для функции $f$ следует, что $\inf(D^v)\neq\varnothing$. Следовательно, существует число $j$ в множестве $\{1,..., m\}$ такое, что $\inf([D^v]_j)=\varnothing$. А так как $\forall v\in V(|D_f^v|=1)$, то $\forall U\subseteq D_f(\inf(f(U))=\varnothing\Rightarrow U\supseteq D^v)$, и, следовательно, $\forall U\subseteq D_f(\inf(f(U))=\varnothing\Rightarrow\inf([U]_j)=\varnothing$, откуда по следствию из леммы 1 имеем $\exists s\in T^{(1)}(f(x_1,..., x_m)\geq s(x_j))$. Лемма доказана.

Пусть $f$ – произвольная квазимонотонная функция. *Весом* функции $f$ будем называть число $W_f=\sum|c|\cdot|D_f^c|$, где суммирование ведется по всем $c$ из $C$.

Так как $\forall s\in S\forall c\in C(|c|=|s(c)|)$, то $\forall s\in S\forall f\in Q(W_f=W_{s(f)})$. Можно показать также, что $f\leq g\Rightarrow W_f\leq W_g$ и $f<g\Rightarrow W_f<W_g$. В дальнейшем будем пользоваться этими фактами без оговорок.

**Лемма 3.** Пусть $f$ – произвольная функция в $Q^{(m)}-\Phi$. Тогда найдется функция $s$ в $S$, найдутся квазимонотонные функции $g_1$ и $g_2$ такие, что $f=s(g_1\vee g_2)$, и $W_f<W_{g1}$, $W_f<W_{g2}$.

Доказательство. Так как $f\notin\Phi$, то $\exists c\in E$ $\exists d_1\in D_f$ $\exists d_2\in D_f$ $(d_1\neq d_2\&f(d_1)\cap c=f(d_2)\cap c=\varnothing)$. Построим функции $f_1$, $f_2$ такие, что $D_{f1}=D_{f2}=D_f$ и $f_1(d_1)=f(d_1)+c$, $f_1(d_2)=f(d_2)$, $f_2(d_1)=f(d_1)$, $f_2(d_2)=f(d_2)+c$ и для каждого $d$ в $D_f-\{d_1,d_2\}$ верно: $f_1(d)=f_2(d)=f(d)$. По построению $f_1>f$ и $f_2>f$, откуда следует, что $f_1,f_2\in Q$, $W_f<W_{f1}$, $W_f<W_{f2}$. Возьмем функцию $s$ в $S$ такую, что $s(0)=c$. Тогда $s(s^{-1}f_1(d_1)\vee s^{-1}f_2(d_1))=s((s^{-1}f(d_1)+0)\vee s^{-1}f(d_1))=ss^{-1}f(d_1)=f(d_1)$, $s(s^{-1}f_1(d_2)\vee s^{-1}f_2(d_2))=s(s^{-1}f(d_2)\vee(s^{-1}f(d_2)+0))=ss^{-1}f(d_2)=f(d_2)$ и для любого $d$ в множестве $D_f-\{d_1,d_2\}$ верно: $s(s^{-1}f_1(d)\vee \vee s^{-1}f_2(d))=s(s^{-1}f(d)\vee s^{-1}f(d))=ss^{-1}f(d)=f(d)$. Следовательно, $f=s(s^{-1}(f_1)\vee s^{-1}(f_2))$.

В качестве функций $g_1$, $g_2$ возьмем функции $s^{-1}(f_1)$ и $s^{-1}(f_2)$ соответственно. Тогда $f=s(g_1\vee g_2)$, $W_f<W_{g1}$, $W_f< <W_{g2}$. Лемма доказана.

*Расширением* квазимонотонной функции $f$ будем называть квазимонотонную функцию $F_f:D_f\to C$ такую, что $F_f(d)=E$, если $\forall e\in E(d\notin\max(M_f^e))$ и $E-\sup\{e:e\in E\ \&d\in\max(M_f^e)\}$ в противном случае.

**Лемма 4.** Пусть $f\in Q$, $g\in M$ и $g\leq F_f$. Тогда $g\leq f$.

Доказательство. Для произвольного элемента $d$ в $D_f$ и произвольного элемента $e$ в $E$ пусть верно: $e\notin f(d)$. Тогда $f(d)\cap e=\varnothing$ и, следовательно, $d\in M_f^e$. Значит, существует элемент $d'\in\max(M_f^e)$ такой, что $d\leq d'$, и по построению функции $F_f$: $e\notin F_f(d')$. А так как $g\leq F_f$, то $e\notin g(d')$. В силу монотонности функции $g$ $g(d)\leq g(d')$ и $e\notin g(d)$. Это доказывает, что $g(d)\leq f(d)$ и в силу произвольности выбора элемента $d$ в $D_f$ $g\leq f$. Лемма доказана.

**Лемма 5.** $\forall f\in Q(f\leq F_f)$.

Доказательство. Пусть $f\in Q$. Для произвольного элемента $d$ в $D_f$ и произвольного элемента $e$ в $E$: если $e\notin F_f(d)$, то $d\in\max(M_f^e)$ и, следовательно, $e\notin f(d)$. Это означает, что $f(d)\leq F_f(d)$. Лемма доказана.

Доказанные выше леммы позволяют нам сформулировать **метод синтеза $r$-формул для функций из $Q$ в базисе $\{\vee\}\cup T^{(1)}$.**

1. Пусть $f$ – квазимонотоная функция, формулу для которой необходимо построить. Построим расширение $F_f$ функции $f$. В соответствии с леммой 5 $f\leq F_f$ и, следовательно, $W(f)\leq W(F_f)$. В соответствии с леммой 4, вследствие монотонности базиса $\{\vee\}\cup T^{(1)}$, $r$-формула для функции $F_f$ является также и $r$-формулой для функции $f$, поэтому далее вместо $r$-формулы для функции $f$ будем строить $r$-формулу для функции $F_f$.

2. Если функция $F_f$ принадлежит множеству $\Phi$, то реализуем ее одноместной функцией из $T^{(1)}$ способом, описанным в доказательстве леммы 2. В противном случае разложим ее по функции $s(x\vee y)$ при некоторой функции $s$ в $S$ способом, описанным в

доказательстве леммы 3, на квазимонотонные компоненты большего веса. С компонентами разложения поступим так же, как и с функцией $f$. Так как количество квазимонотонных функций любой конечной местности конечно, то через конечное число разложений получим формулу над $\{\vee\}\cup T^{(1)}$, реализующую функцию $f$.

. Описанный метод синтеза является доказательством теоремы 1.

**Теорема 1.** Система функций $\{\vee\}\cup T^{(1)}$ $r$-полна в $Q$.

Для произвольного числа $l$ в $\{0,..,k\}$ введем специальный класс $\Phi_l$ квазимонотонных функций, определив его при $l\neq 0$ выражением $\Phi_l=\{f\in Q\colon \exists c\in C(|c|=l \& \forall e\in c(|M_f^e|\leq 1))\}$ и положив $\Phi_0=Q$.

Справедливо включение: $\Phi_0\supseteq\Phi_1\supseteq\ldots\supseteq\Phi_k=\Phi$. Заметим, что $\forall s\in S(f\in\Phi_l\Rightarrow s(f)\in\Phi_l)$ и $(g\leq f \& g\in\Phi_l)\Rightarrow f\in\Phi_l$.

**Лемма 6.** Пусть $f$ – произвольная функция из $\Phi_l$, при некотором $l<k$. Тогда существует функция $s$ в $S$, существуют функции $f_1,\ldots,f_r$ в множестве $\Phi_{l+1}$ такие, что $f=s(f_1\vee\ldots\vee f_r)$.

Доказательство. Так как $f\in\Phi_l$, то существует элемент $c$ в $C$ такой, что $|c|=l$ и для каждого элемента $e$ из $c$ верно $|M_f^e|\leq 1$. Пусть $j$ – произвольный элемент из $E-c$. Пусть $M_f^j=\{d_1,\ldots,d_r\}$, $r>1$. Построим функции $g_1,\ldots,g_r$ такие, что $D_{g1}=D_{g2}=\ldots=D_{gr}=D_f$, для произвольного $i$ в $\{1,\ldots,r\}$, положив $g_i(d)=f(d)+j$, если $d\in M_f^j-d_i$, и $g_i(d)=f(d)$, если $d\notin M_f^j-d_i$. Так как $\forall i\in\{1,\ldots,r\}\forall e\in(c+j)(|M_{gr}^e|\leq 1)$ и $|c+j|=l+1$, то $g_1,\ldots,g_r\in\Phi_{l+1}$.

Пусть $s$ – произвольная функция из $S$ такая, что $s(0)=j$. Для каждого $i$ из $\{1,\ldots,r\}$ возьмем в качестве функции $f_i$ композицию функций $s^{-1}(g_i)$. Можно показать, что справедливо представление $f=s(f_1\vee\ldots\vee f_r)$. А так как функции $g_1,\ldots,g_r$ принадлежат множеству $\Phi_{l+1}$, то и функции $f_1,\ldots,f_r$ принадлежат $\Phi_{l+1}$. Лемма доказана.

Лемма 6 дает нам еще один **метод синтеза $r$-формул для функций из $Q$ в базисе $\{\vee\}\cup T^{(1)}$.**

1. Пусть $f$ – квазимонотонная функция, формулу для которой необходимо построить. Построим расширение $F_f$ функции $f$. В соответствии с леммой 5 $f\leq F_f$, следовательно, если для некоторого $l$ верно $f\in\Phi_l$, то верно и $F_f\in\Phi_l$. Вместо $r$-формулы для функции $f$ будем строить $r$-формулу для функции $F_f$.

2. Если функция $F_f$ принадлежит множеству $\Phi_0$, то реализуем ее одноместной функцией из $T^{(1)}$ способом, описанным в доказательстве леммы 2. В противном случае функция $F_f$ принадлежит множеству $\Phi_l$ при некотором $l<k$. Разложим ее по функции $s(x\vee y)$ при некоторой $s$ из $S$ способом, описанным в доказательстве леммы 6, на квазимонотонные компоненты из $\Phi_{l+1}$. С компонентами разложения поступим так же, как и с функцией $f$. Через конечное число разложений получим формулу над $\{\vee\}\cup T^{(1)}$, реализующую $f$.

## Синтез $s$-формул для квазимонотонных функций в базисах, содержащих функции из $\{\vee\}\cup T^{(1)}$

Введем в рассмотрение специальный класс $B$ квазимонотонных функций, определив его при помощи выражения $f\in B\Leftrightarrow\exists e\in E\exists c\in C(e<c \& V_f=\{e,c\} \& |D_f^c|=1)$. Для любой функции $s$ из $S$ определим операцию $\vee_s$ следующим образом: $x\vee_s y=s^{-1}(sx\vee sy)$.

**Лемма 7.** Пусть $f,f_0\in Q$ и $f\geq f_0$. Существуют функции $s_1,\ldots,s_r$ из $S$ и функции $f_1,\ldots,f_r$ из $B$ такие, что $f=f_0\vee_{s1}f_1\vee_{s2}f_2\ldots\vee_{sr}f_r$.

Доказательство. Случай $f=f_0$ тривиален. Пусть $f\neq f_0$. Тогда $f>f_0$. Положим $D_0=\{d\in D_f: f(d)>f_0(d)\}$. Пусть $D_0=\{d_1,\ldots,d_r\}$. Зафиксируем указанную нумерацию элементов в $D_0$. Для каждого $i$ из $\{1,..,r\}$ пусть $e_i$ – произвольный элемент множества $f_0(d_i)$. Для каждого элемента $i$ из $\{1,\ldots,r\}$ построим функцию $f_i:D_f\to\{e_i,f(d_i)\}$ из $B$, положив $f_i(d)=f(d)$, если $d=d_i$ и $f_i(d)=e_i$ для любого $d\in D_f-d$. При любом $i$ из $\{1,\ldots,r\}$ пусть $s_i$ – функция из $S$ такая, что $s_i(e_i)=0$. Для любого $D\subseteq D_f$ постоим функцию $f^D:D_f\to V_f$, положив $f^D(d)=f(d)$, если $d\in D$, и положив $f^D(d)=f_0(d)$, в противном случае. Заметим, что $f^D=f$ при $D=D_0$ и $f^D=f_0$. Пусть $D\subseteq D_0-d_i$ для некоторого $i$ в $\{1,\ldots,r\}$. Тогда $f^{D\cup di}=f^D\vee_{si}f_i$. Покажем это.

Если $d\in D$, то $f^D(d)=f(d)$, $f_i(d)=e_i$ и, следовательно,

$$s_i^{-1}(s_if^D(d)\vee s_if_i(d))=s_i^{-1}(s_if(d)\vee s_ie_i)=s_i^{-1}(s_if(d)\vee 0)=$$
$$=s_i^{-1}(s_if(d))=f(d)=f^{D\cup di}(d).$$

Если $d\in D_f-(D\cup d_i)$, то $f^D(d)=f_0(d)$, $f_i(d)=e_i$ и, следовательно

$$s_i^{-1}(s_if^D(d)\vee s_if_i(d))=s_i^{-1}(s_if_0(d)\vee s_ie_i)=s_i^{-1}(s_if_0(d)\vee 0)=$$
$$=s_i^{-1}(s_if_0(d))=f_0(d)=f^{D\cup di}(d).$$

Если $d=d_i$, то $f^D(d)=f_0(d)=f_0(d_i)\geq e_i$ и $f_i(d)=f(d)=f(d_i)\geq f_0(d_i)\geq e_i$ и, следовательно, с одной стороны

$$s_i^{-1}(s_if^D(d)\vee s_if_i(d))\leq s_i^{-1}(s_if^D(d)+s_if_i(d))=f^D(d)+f_i(d)=$$
$$=f_0(d_i)+f_i(d_i)=f_i(d_i)=f(d)=f^{D\cup di}(d),$$

. . . .

а с другой стороны,

$$s_i^{-1}(s_if^D(d)\vee s_if_i(d))\geq s_i^{-1}(s_ie_i\vee s_if_i(d))=s_i^{-1}(0\vee s_if_i(d))=f_i(d)=f^{D\cup di}(d).$$

Итак, имеем $f^{D\cup di}=f^D\vee_{si}f_i$, откуда следует:

$$f^{d1}=f_0\vee_{s1}f_1,\ f^{d1\cup d2}=f_0\vee_{s1}f_1\vee_{s2}f_2,\ \ldots.$$
$$f=f^{d1\cup d2\cup\ldots\cup dr}=f_0\vee_{s1}f_1\vee_{s2}f_2\ldots\vee_{sr}f_r.$$

Лемма доказана.

**Лемма 8.** Пусть $f$ – произвольная функция из $B^{(m)}$. Тогда существуют функции $s_0,\ldots,s_m$ в $B^{(1)}$ такие, что $f(x_1,\ldots,x_m)=s_0(s_1x_1\vee\ldots\vee s_mx_m)$.

Доказательство. Так как $f$ – функция в $B$, то существуют элементы $e$ в $E$, $c$ в $C$, $d=(d_1,\ldots,d_m)$ в $D_f$ такие, что $e<c$ и $f$ принимает значение $e$ на всех аргументах, кроме $d$, на котором она равна $c$. Для произвольных элементов $h$ из $C$, $a$ из $E$, $b$ из $C$ таких, что $a<b$, обозначим $\varphi_h^{a,b}$ функцию из $B^{(1)}$, которая принимает значение $b$ при аргументе, равном $h$, и значение $a$ при остальных значениях аргумента.

Пусть $h=\{k-1,0\}$ – элемент из $C$. Положим $s_0=\varphi_h^{e,c}$ и $s_i=\varphi_{di}^{k-1,h}$ для каждого $i$ из $\{1,\ldots,m\}$. Можно показать, что $f(x_1,\ldots,x_m)=s_0(s_1x_1\vee\ldots\vee s_mx_m)$. Лемма доказана.

Леммы 7, 8 позволяют нам сформулировать следующий **метод синтеза $s$-формул для функций из $Q$ в базисе $\{\vee\}\cup T^{(1)}\cup B^{(1)}$.**

1. Любым известным способом получим реализацию $f_0$ функции $f$ в базисе $\{\vee\}\cup T^{(1)}$.

2. Способом, описанным в доказательстве леммы 7, находим функции $s_1,\ldots,s_r$ в $T^{(1)}$ и функции $f_1,\ldots,f_r$ в $B$ и представляем $f$ в форме $f=f_0\vee_{s1}f_1\vee_{s2}f_2\ldots\vee_{sr}f_r$.

3. Способом, описанным в доказательстве леммы 8, для каждой $f_i$ из $f_1,\ldots,f_r$ находим функции $s_{0,i},\ldots,s_{m,i}$ в $B^{(1)}$ такие, что $f_i(x_1,\ldots,x_m)=s_{0,i}(s_{1,i}(x_1)\vee\ldots\vee s_{m,i}(x_m))$, и представляем $f$ в форме $f=f_0\vee_{s1}f_1\vee_{s2}f_2\ldots\vee_{sr}f_r=f_0\vee_{s1}[s_{0,1}(s_{1,1}(x_1)\vee\ldots\vee s_{m,1}(x_m))]\vee_{s2}\vee_{s2}[s_{0,2}(s_{1,2}(x_1)\vee\ldots\vee s_{m,2}(x_m))]\ldots\vee_{sr}[s_{0,r}(s_{1,r}(x_1)\vee\ldots\ldots\vee s_{m,r}(x_m))]$.

Следствием теоремы 1 и данного метода синтеза является следующая теорема.

**Теорема 2.** Система функций $\{\vee\}\cup T^{(1)}\cup B^{(1)}$ $s$-полна в $Q$.

## Синтез $s$-формул для монотонных функций в базисах, содержащих функции из $\{\vee\}\cup T^{(1)}$

Введем в рассмотрение специальный класс $B_M$ монотонных функций: произвольная функция $f$ из $M$ принадлежит $B_M$, если и только если найдутся элементы $e$ в $E$, $c$ в $C$ и $d$ в $D_f$ такие, что $e<c$, $V_f=\{e, c\}$ и для любого элемента $d'$ из $D_f$ верно $f(d')=c \Leftrightarrow d'\geq d$.

Для произвольных $e$ из $E$, $c$ из $C$ таких, что $e<c$, и для произвольного $d$ из $C^m$ при некотором $m$ обозначим $f_d^{e,c}$ функцию из $B_M$, определенную на $C^m$, такую, что для каждого $d'$ из $C^m$: $f(d')=c$ если $d'\geq d$, и $f(d')=e$ в противном случае.

**Лемма 9.** Пусть $f, f_0$ – функции из $M$ и $f\geq f_0$. Тогда найдется число $r$, функции $s_1,..., s_r$ из $S$ и функции из $f_1,..., f_r$ из $B_M$ такие, что $f=f_0\vee s_1f_1\vee s_2f_2...\vee s_rf_r$.

Доказательство. Случай $f=f_0$ – тривиален. Пусть $f\neq f_0$. Тогда $f>f_0$. Обозначим $D_0=\{d\in D_f | f(d)>f_0(d)\}$. Пусть $D_0=\{d_1,..., d_r\}$. Зафиксируем указанную нумерацию элементов в $D_0$. Для произвольного $i$ в $\{1,..., r\}$ пусть $e_i$ – произвольный элемент из множества $f_0(d_i)$ и $h_i=f(d_i)$. Для каждого элемента $i$ из $\{1,..., r\}$ возьмем функцию $f_i: D_f\to\{e_i, h_i\}$ в $B_M$ такую, что $f_i=f_{di}^{ei, hi}$. Пусть при любом $i$ из $\{1,..., r\}$ $s_i$ – функция из $S$ такая, что $s_i(e_i)=0$. Для любого $D\subseteq D_f$ построим функцию $f^D: D_f\to V_f$ для произвольного $d'$ в $D_f$, положив $f^D(d')=f_0(d')+\sum f_i(d)$, где суммирование ведется по всем $d$ из $D$, содержащимся в элементе $d'$. Заметим, что $f^D=f$ при $D=D_0$ и $f^{\varnothing}=f_0$. Пусть $i\in\{1,..., r\}$ и $D\subseteq D_0-d_i$. Тогда $f^{D\cup di}=f^D\vee s_if_i$. Покажем это.

Пусть $d\in D_f$ и $d$ не реализуется $d_i$. Тогда $f_i(d)=e_i$ и, следовательно, $f^D\vee s_if_i=s_i^{-1}(s_if^D(d)\vee s_if_i(d))=s_i^{-1}(s_if^D(d)\vee s_ie_i)=s_i^{-1}(s_if^D(d)\vee 0)=s_i^{-1}(s_if^D(d))=f^D(d)=f^{D\cup di}(d)$. Пусть $d\geq d_i$. Тогда $f_i(d)=h_i>e_i$, $f^D(d)\geq f_0(d)\geq f_0(d_i)=h_i>e_i$ и $f^D(d)\vee s_if_i(d)=s_i^{-1}(s_if^D(d)\vee s_if_i(d))\leq s_i^{-1}(s_if^D(d)+s_if_i(d))=f^D(d)+f_i(d)=f^D(d)+f(d)=f^{D\cup di}(d)$. С другой стороны, так как $f^D\vee s_if_i=s_i^{-1}(s_if^D(d)\vee s_if_i(d))\geq s_i^{-1}\times\times(s_ie_i\vee s_if_i(d))\geq s_i^{-1}(0\vee s_if_i(d))=f_i(d)$ и $f^D\vee s_if_i=s_i^{-1}(s_if^D(d)\vee\vee s_if_i(d))\geq s_i^{-1}(s_if^D(d)\vee s_ie_i)\geq s_i^{-1}(s_if^D(d)\vee 0)=f^D(d)$, то $f^D(d)\vee s_if_i(d)\geq f^D(d)+f_i(d)=f^D(d)+f(d)=f^{D\cup di}(d)$. Следовательно, $f^D(d)\vee\vee s_if_i(d)=f^{D\cup di}(d)$, откуда получаем: $f^{d1}=f_0\vee s_1f_1, f^{d1\cup d2}=f_0\vee\vee s_1f_1\vee s_2f_2,... f=f^{d1\cup d2\cup...\cup dr}=f_0\vee s_1f_1\vee s_2f_2...\vee s_rf_r$. Лемма доказана.

**Лемма 10.** Пусть $f$ – произвольная функция из $B_M^{(m)}$. Тогда существуют функции $s_0,..., s_m$ в $B_M^{(1)}$ такие, что $f(x_1,..., x_m)=s_0(s_1x_1\vee...\vee s_mx_m)$.

Доказательство. $f\in B_M$, поэтому существуют элементы $e$ в $E$, $c$ в $C$, $d=(d_1,..., d_m)$ в $D_f$ такие, что $e<c$ и $f$ принимает значение $c$ на аргументах, реализуемых $d$, и значение $e$ на остальных аргументах.

Пусть $h=\{k-1,0\}$ – элемент из $C$. Положим $s_0=f_h^{e, c}$ и $s_i=f_{di}^{k-1, h}$ для всех $i\in\{1,..., m\}$. Можно показать, что $f(x_1,..., x_m)=s_0(s_1x_1\vee...\vee s_mx_m)$. Лемма доказана.

Леммы 9, 10 позволяют нам сформулировать следующий **метод синтеза $s$-формул для функций из $M$ в базисе $\{\vee\}\cup T^{(1)}\cup B_M^{(1)}$**.

1. Любым известным способом получим реализацию $f_0$ функции $f$.

2. Способом, описанным в доказательстве леммы 9, находим функции $s_1,..., s_r$ в $T^{(1)}$, функции в $f_1,..., f_r$ из $B_M$ и представляем $f$ в форме $f=f_0\vee s_1f_1\vee s_2f_2...\vee s_rf_r$.

3. Способом, описанным в доказательстве леммы 10, для каждой $f_i$ из $f_1,..., f_r$ находим функции $s_{0,i}, ..., s_{m,i}$ в $B^{(1)}$ такие, что $f_i(x_1,..., x_m)=s_{0,i}(s_{1,i}(x_1)\vee...\vee s_{m,i}(x_m))$, и представляем функцию $f$ в форме $f=f_0\vee s_1f_1\vee s_2f_2...\vee s_rf_r=$ $=f_0\vee s_1[s_{0,1}(s_{1,1}(x_1)\vee...\vee s_{m,1}(x_m))]\vee s_2[s_{0,2}(s_{1,2}(x_1)\vee...\vee s_{m,2}(x_m))]$ $...\vee s_r[s_{0,r}(s_{1,r}(x_1)\vee...\vee s_{m,r}(x_m))]$.

Описанный метод синтеза является доказательством следующей теоремы.

**Теорема 3.** Система функций $\{\vee\}\cup T^{(1)}\cup B_M^{(1)}$ $s$-полна в $M$.

ЛИТЕРАТУРА


1. *Агибалов Г.П.* Дискретные автоматы на полурешетках. Томск: Изд-во Том. ун-та, 1993. 227 с.
2. *Агибалов Г.П.* О полных системах операций и синтезе схем для квазимонотонных функций на конечных полурешетках // Новые информационные технологии в исследовании дискретных структур. Екатеринбург: Из-во УрО РАН, 1998. С. 149–152.
3. *Агибалов Г.П.* О полных системах функций на полурешетке подмножеств конечного множества // Всесибирские чтения по математике и механике: Математика. Томск: Изд-во Том. ун-та, 1997. Т. 1. С. 148–149.
4. *Агибалов Г.П.* К синтезу схем, реализующих квазимонотонные функции на полурешетке подмножеств двухэлементного множества. // Там же. С. 147–148.



Статья представлена кафедрой защиты информации и криптографии факультета прикладной математики и кибернетики Томского государственного университета, поступила в научную редакцию 1 марта 2000 г.

УДК 621.391.7



*И.В. Пронина, Г.П. Агибалов*


# НЕКОТОРЫЕ АЛГОРИТМЫ КРИПТАНАЛИЗА ДЛЯ КОДОВЫХ КРИПТОСИСТЕМ


Предлагаются алгоритмы криптанализа для кодовых криптосистем с закрытым ключом с целью нахождения ключа при возможности выбора сообщений и для кодовых криптосистем с открытым ключом с целью нахождения сообщения, если известны открытый ключ и криптограмма.


## Введение

Кодовые криптосистемы строятся на основе линейных кодов, исправляющих ошибки. Как и все криптосистемы, они делятся на два класса – симметричные, или с закрытым ключом, и несимметричные, или с открытым ключом. Криптанализу последних посвящены работы [1, 2, 3], где для некоторых кодовых криптоси-