ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXIX 1979 2

УДК 517.11

МАТЕМАТИКА

Г. А. Назарян

О дизъюнктных разбиениях множеств булевых функций

(Представлено чл.-корр. АН Армянской ССР В. В. Варшамовым 29/V 1979)

Пусть задано множество M. Разбиением этого множества, как обычно, будем называть семейство попарно непересекающихся подмножеств множества M такое, что сумма всех подмножеств этого семейства равна M. Для каждого заданного разбиения каждое подмножество, принадлежащее разбиению, будем называть смежным классом. При $M' \subseteq M$ разбиение M будем называть дизъюнктным по отношению к множеству M', если никакие два различных элемента из M' не попадают в один и тот же смежный класс этого разбиения.

В дальнейшем нас будут интересовать дизъюнктные разбиения множеств булевых функций. Мы покажем, что существует прямая связь между сложностью алгоритмического задания дизъюнктных разбиений множеств булевых функций и сложностью алгоритмов синтеза, определенных для этих множеств.

1. В дальнейшем будем использовать следующие сокращения и обозначения: б. ф.—булева функция, н. ч.—натуральное число, о. р. ф.—общерекурсивная функция, ч. р. ф.—частично рекурсивная функция. Слова в $\{0, 1\}$ естественным образом будем отождествлять с н. ч. ([1]). Длину н. ч. x будем обозначать посредством $l(x)$. Если Q есть конечное множество н. ч., то через $\overline{Q}$ будем обозначать мощность этого множества. Размерность б. ф. будем указывать верхним индексом, так что если F есть б. ф. размерности n (т. е. слово в $\{0, 1\}$ длины 2^n, содержащее информацию о всех значениях F), то будем писать F^n. Букву B будем использовать для обозначения множества всех б. ф., букву M—в качестве переменной для обозначения произвольного перечислимого множества б. ф. (при этом посредством M_n будем обозначать множество б. ф. размерности n, принадлежащих M), букву C—для обозначения н. ч., буквы T и t—для обозначения одноместных о. р. ф. и букву H—для обозначения двухместных о. р. ф. Символ λ_M используем для обозначения характеристической функции множества M.

Будем предполагать фиксированным некоторое положительное рациональное число $\varepsilon < 1/2$, относительно которого рассматриваются все приближения б. ф. Все вводимые далее определения и обозначения, относящиеся к приближенным вычислениям и содержащие ε, мы будем употреблять и при рассмотрении точных вычислений ($\varepsilon = 0$); при этом, сохраняя обозначения, будем употреблять их без ε. Буквами r и ρ будем обозначать такие функции, что для слов a и a' в $\{0, 1\}$ одинаковой длины $r(a, a')$ есть расстояние по Хеммингу между a и a' (т. е. число компонент, в которых a и a' различаются) и $\rho(a, a') = r(a, a')/l(a)$. Если $\rho(a, a') < \varepsilon$, то будем писать $a \overset{\cdot}{=} a'$ и говорить, что a и a' ε-равны. При сравнении функций α и β символы $<$ и $\overset{\cdot}{=}$ будем использовать в следующем смысле: $(\alpha <\cdot \beta) \equiv \exists C \forall n (\alpha(n) < \beta(n) + C)$, $(\alpha \overset{\cdot}{=} \beta) \equiv (\alpha <\cdot \beta) \& (\beta <\cdot \alpha)$.

В качестве основного алгоритмического языка будем рассматривать некоторую аддитивно оптимальную нумерацию ч. р. ф. ([2,3]) φ, т.е. такую нумерацию одноместных ч. р. ф., что для любой другой нумерации одноместных ч.р.ф. ψ можно указать о.р.ф. ν такую, что $\forall i \forall n ((\varphi_{\nu(i)} = \psi_i) \& \& l(\nu(i)) <\cdot l(i)))$. Будем говорить, что ч. р. ф. α вычисляет б. ф. F^n, если $\forall x (l(x) = n \supset \alpha(x) = F^n(x))$, и что ч. р. ф. α ε-вычисляет F^n (и писать $\alpha \overset{\cdot}{\Rightarrow} F^n$), если α вычисляет б. ф., ε-равную F^n. Для нумерации φ зафиксируем последовательность Φ, сигнализирующих ([4]), и с каждой Φ_p ассоциируем ч. р. ф. $\hat{\Phi}_p$ такую, что $\forall n (\hat{\Phi}_p(n) = \max_{l(x)=n} \Phi_p(x))$. Под ε-алгоритмом синтеза будем понимать произвольную о. р. ф. (будем использовать сокращение ε-а. с.), под областью применимости ε-а. с. A будем понимать множество $D^A = \{F | \varphi_{A(F)} \overset{\cdot}{\Rightarrow} F\}$. Если A есть ε-а. с., то посредством $|A(F^n)|^{-1}$ будем обозначать множество $\{\bar{F}^n | A(\bar{F}^n) = A(F^n)|$. Будем говорить, что A есть ε-а. с. для M, если $M \subseteq D^A$, при этом псевдофункцией Шеннона ([1]) M по A будем называть такую псевдофункцию $L^{\cdot}_{M,A}$, что $\forall n (L^{\cdot}_{M,A}(n) = \max_{F^n \in M_n} l(A(F^n)))$. Посредством $L^{\cdot}_{M}$ будем обозначать псевдофункцию Шеннона множества M, понимаемую естественным образом, а именно $L^{\cdot}_{M}(n) = \max(\min l(p) | \varphi_p \overset{\cdot}{\Rightarrow} F^n)$, где максимум берется по б. ф. размерности n, принадлежащим M. ε-а. с. A будем называть оптимальным для M, если $L^{\cdot}_{M,A} \overset{\cdot}{=} L^{\cdot}_{M}$. Посредством $L^{\cdot,T}$ будем обозначать такую ч. р. ф., что $\forall n \forall F^n (L^{\cdot,T}(F^n) = l(\min\{p | \varphi_p \overset{\cdot}{\Rightarrow} F^n) \& (\hat{\Phi}_p(n) < T(n))\})$. Пусть a есть булев вектор; множество векторов той же длины, что и a, ε-равных a, будем называть шаром радиуса ε с центром a. Под ε-мощностью множества Q (ее будем обозначать через $d^{\cdot}(Q)$) б. ф. одинаковой размерности будем понимать минимальное число шаров радиуса ε, достаточное для покрытия Q.

Будем рассматривать такие разбиения Ω множества B, что каждый смежный класс содержит б. ф. одной и той же размерности. Такие разбиения индуцируют разбиения B_n, которые будем обозначать посредством Ω_n, а их мощность посредством $\overline{\Omega}_n$. Будем предполагать, что рассматриваемые разбиения рекурсивны, а именно, что для каждого разбиения Ω существует рекурсивная „n-характеристическая функция" f, удовлетворяющая условию: для всякого n, для любых y и z, принадлежащих B_n, равенство $f(n, y)=f(n, z)$ имеет место тогда и только тогда, когда y и z принадлежат одному и тому же смежному классу разбиения B_n. Для удобства будем предполагать, что разбиение задается одноместной рекурсивной функцией f такой, что $\forall n \forall F^n(f(F^n)=f(n,F^n))$. Разбиение Ω множества B будем называть дизъюнктным по отношению к M, если в каждом смежном классе разбиения Ω содержится не более одного элемента из M. Разбиение Ω, дизъюнктное по отношению к M, будем для краткости называть дизъюнктом M. Разбиение Ω множества B будем называть ε-дизъюнктом M, если б. ф. из M, принадлежащие произвольному смежному классу этого разбиения, содержатся в некотором шаре радиуса ε. Разбиение Ω множества B будем называть конструктивным ε-дизъюнктом множества M, если оно является ε-дизъюнктом и существует частичный алгоритм, который по элементу всякого смежного класса, имеющего непустое пересечение с M, выдает центр шара радиуса ε, в котором содержатся все б. ф. этого пересечения. Нетрудно убедиться в том, что ε-дизъюнкты рекурсивных множеств конструктивны. ε-дизъюнкт Ω (соответственно ε-а. с. A) будем называть T-ε-дизъюнктом (T-ε-а. с.), если можно указать программу φ_p, вычисляющую характеристическую функцию разбиения Ω (вычисляющую ε-а. с. A) такую, что $\forall_n^{\infty}(\hat{\Phi}_p(2^n) < T(n))$; для обозначения указанных фактов будем использовать также записи $\Omega \in R_T$, соответственно $A \in R_T$, а также $\lambda_M \in R_T$, для обозначения аналогичного факта для λ_M.

2. Рассмотрения этого пункта относятся к случаю $\varepsilon = 0$. Последующие два утверждения иллюстрируют существование множеств б. ф., существенно отличающихся по мощности от своих дизъюнктов (примеры множеств, для которых существуют равномощные им дизъюнкты, нетрудно построить).

2.1. *Для любой монотонной неограниченной о. р. ф. a (сколь угодно медленно растущей) можно указать перечислимое множество M такое, что $\forall n(\overline{M}_n < a(n))$ и для всякого дизъюнкта Ω множества M имеет место $\forall_n^{\infty}(\Omega_n = B_n)$.*

Следующее утверждение является рекурсивным аналогом 2.1.

2.2. *Для любой монотонной неограниченной о. р. ф. a (сколь угодно медленно растущей) и для любой о. р. ф. T можно указать рекурсивное M такое, что $\forall n(\overline{M}_n < a(n))$ и для всякого T-дизъюнкта Ω множества M имеет место $\forall_n^{\infty}(\Omega_n = B_n)$.*

Следующая теорема показывает, что сложность (например, время работы) оптимальных а. с. для множеств находится в прямой зависимости от сложности задания разбиения дизъюнктов множеств, близких к ним по мощности.

Теорема 1. *Можно указать о. р. ф. H такую, что для всякого перечислимого M и для всякой о. р. ф. T выполнено:*

(а) *по всякому T-дизъюнкту Ω множества M можно указать а. с. A для M такой, что*

$$L_{M,A}(n) < l(\overline{\Omega}_n) \text{ и } A \in R_{H(n,T(n))};$$

(б) *по всякому T-а. с. A для M можно указать дизъюнкт Ω множества M такой, что*

$$l(\overline{\Omega}_n) < L_{B,A}(n) \text{ и } \Omega \in R_{H(n,T(n))},$$

если $\lambda M \in R_T$, то можно указать дизъюнкт Ω множества M такой, что

$$l(\overline{\Omega}_n) < L_{M,A} \text{ и } \Omega \in R_{H(n,T(n))}.$$

Согласно пункту (б) теоремы, для множеств со сложной характеристической функцией мощность дизъюнкта является нижней оценкой функции $L_{B,A}$, а не $L_{M,A}$. Как показывает следующее утверждение, нижняя оценка для $L_{B,A}$ является нижней оценкой для $L_{M,A}$ для многих n.

2.3. Для любых перечислимого множества M и о. р. ф. $\gamma(n) < 2^n$ выполнено: $[\forall(\text{а. с. } A \text{ для } M)\forall_n^\infty(L_{B,A}(n) > \gamma(n))] \supset [\forall(\text{а. с. } A \text{ для } M)\exists_n^\infty(L_{M,A}(n) > \gamma(n))]$.

Из теоремы и утверждений 1, 2 и 3 следует существование множеств, либо вовсе не допускающих оптимальных а. с., либо не допускающих просто вычислимых оптимальных а. с.

Из теоремы также следует, что сложность а. с. для множеств б. ф. не определяется сложностью б. ф., из которых эти множества составлены; а именно, множество может быть составлено из сложных б. ф., но допускать просто вычислимый оптимальный а. с. Этот факт вытекает из теоремы посредством следующего рассуждения: разобьем (некоторым простым способом) для каждого n множество B_n на n подмножеств $Q_n^1, Q_n^2, \ldots, Q_n^n$ равной мощности $(l(Q_n^i) = 2^n - l(n))$, далее из каждого множества Q_n^i выберем сложную б. ф. (например, такую, что при достаточно большом ограничении T на время работы программ эта б. ф. вычисляется лишь программами объема больше чем $2^n - l(n)$); множество выбранных таким образом б. ф. объявим множеством б. ф. размерности n некоторого множества M; существование просто вычислимого оптимального а. с. для этого множества следует из возможности простого разбиения B_n. Таким образом имеет место следующее утверждение (оно нам понадобится и для последующих рассмотрений).

2. 4. *Можно указать такую о. р. ф. t, что для всякой о. р. ф. T существует множество M мощности $\overline{M}_n=n$, удовлетворяющее условию $\forall n\forall(F^n\in M_n)(L^T(F^n)\geqslant 2^n-t(n))$ и обладающее оптимальным t-а. с.*

Как показывает следующее утверждение, если простой а. с. A синтезирует оптимальную программу для сложной б. ф. F, то мощность множества $|A(F)|^{-1}$ будет достаточно велика.

2. 5. $\exists H$ Va. c. $\varphi_z\forall n\forall(F^n\in D^{\varphi_z})(t(d[\varphi_z(F^n)]^{-1})>L^{H(n,\hat{\Phi}_z(2^n))}(F^n)-2t(\varphi_z(F^n))-C)$.

3. В этом пункте рассмотрим случай $\varepsilon\neq 0$. Утверждения этого пункта представляют собой аналоги утверждений пункта 2. Обозначение ω_ε используется для следующей функции: $\omega_\varepsilon(n)=2^n-\log\sum_{i=0}^{[\varepsilon\cdot 2^n]}C^i_{2^n}$, содержательно эта функция для всякого n задает логарифм ε-мощности B_n.

3. 1. *Для любой монотонной неограниченной о. р. ф. a (сколь угодно медленно растущей) можно указать перечислимое M такое, что $\forall_n(d^*(M_n)<a(n))$ и для всякого ε-дизъюнкта Ω множества M выполнено $\forall_n^\infty(\overline{\Omega}_n>\omega_{2\varepsilon}(n))$.*

3.2. *Для любой монотонной неограниченной о. р. ф. a (сколь угодно медленно растущей) и для всякой о. р. ф. T можно указать рекурсивное M такое, что $\forall n(d^*(M_n)<a(n))$ и для всякого T-ε-дизъюнкта Ω множества M выполнено $\forall_n^\infty(\overline{\Omega}_n>\omega_{2\varepsilon}(n))$.*

Теорема 2. *Можно указать о. р. ф. H такую, что для всякого перечислимого M и для всякой о. р. ф. T выполнено:*

(а) *по всякому конструктивному T—ε-дизъюнкту Ω множества M можно указать ε-а. с. A для M такой, что*

$$L^*_{M,A}(n)<\cdot\, l(\overline{\Omega}_n)\ \text{и}\ A\in R_{H(n,T(n))};$$

(б) *по всякому T-ε-а. с. A для M можно указать конструктивный ε-дизъюнкт Ω множества M такой, что*

$$l(\overline{\Omega}_n)<\cdot\, L^*_{B,A}(n)\ \text{и}\ \Omega\in R_{H(n,T(n))};$$

если $\iota_M\in R_T$, то можно указать ε-дизъюнкт Ω множества M такой, что

$$l(\overline{\Omega}_n)<\cdot\, L^*_{M,A}\ \text{и}\ \Omega\in R_{H(n,T(n))}.$$

3. 3. $\forall M\forall\gamma<\omega_\varepsilon|\forall(\varepsilon\text{-а. с. } A \text{ для } M)\,\forall_n^\infty(L^*_{B,A}(n)>\gamma(n))|\supset|\forall(\varepsilon\text{-а.с. } A \text{ для } M)\exists_n^\infty(L^*_{M,A}(n)>\gamma(n))|$.

3. 4. Можно указать о. р. ф. t такую, что для всякой о. р. ф. T существует множество M такое, что $d^*(M_n)=n$, удовлетворяющее условию $\forall n\forall(F^n\in M)(L^{*,T}(F^n)>\omega_\varepsilon(n)-t(n))$ и обладающее оптимальным t-ε-а. с.

3.5. $\exists H \forall \varepsilon$-э с. $\varphi_z \forall n \forall (F^n \in D^{\varphi_z})(l((d')^{-1}|\varphi_z(F^n)|) > L^{\varepsilon, H(n, \hat{\Phi}_{\varphi_z}(2^n))}(F^n) - 2l(\varphi_z(F^n)) - C)$.

4. В этом пункте мы рассмотрим а. с. частного типа, эти а. с. будем называть T-оптимальными. А именно, ε-а. с. A для M будем называть T-оптимальным, если выполнено: для б. ф. из M этот а. с. синтезирует программы, которые не хуже по объему T-минимальных программ, т. е. $\forall n \forall (F^n \in M)|(\varphi_{A(F)} \Rightarrow F) \& (l(A(F^n)) < \min l(p)|(\varphi_p \Rightarrow F^n) \& (\hat{\Phi}_p(n) < T(n)))|$. При $\varepsilon = 0$ данное определение соответствует случаю точных вычислений. Примером T-оптимальных а. с., как нетрудно убедиться, могут служить а. с. из утверждений 2.3 и 3.3; указанные а. с. просто вычислимы и в то же время являются оптимальными для сложных множеств (множеств с трудно вычислимой характеристической функцией). Как показывают следующие утверждения, T-оптимальные а. с. могут быть просто вычислимыми только для множеств со сложной характеристической функцией.

4.1. *Можно указать о. р. ф. H такую, что для всякого рекурсивного M такого, что $\overline{M}_n \to \infty$, и для всякой о. р. ф. T выполнено: если φ_p и φ_q суть соответственно T-оптимальный а. с. для M и характеристическая функция M, то $\forall^{\infty}_n (H(n, \max(\hat{\Phi}_p(2^n), \hat{\Phi}_q(2^n))) > T(n))$.*

4.2. *Можно указать о. р. ф. H такую, что для всякого рекурсивного M такого, что $d'(M_n) \to \infty$, и для всякой о. р. ф. T выполнено: если φ_p и φ_q суть соответственно T-оптимальный ε-а. с. для M и характеристическая функция M, то $\forall^{\infty}_n (H(n, \max(\hat{\Phi}_p(2^n), \hat{\Phi}_q(2^n))) > T(n))$.*

Пользуюсь случаем выразить глубокую благодарность И. Д. Заславскому за внимание и ряд существенных замечаний при написании работы.

Вычислительный центр
Министерства автомобильного транспорта
Армянской ССР

Հ. Հ. ՆԱՋԱՐՅԱՆ

Բուլյան ֆունկցիաների բազմությունների դիզյունկտ տրոհումների մասին

Բոլոր բուլյան ֆունկցիաների (բ. ֆ.) բազմության տրոհումը կանվանենք դիզյունկտ բ. ֆ. M բազմության նկատմամբ, եթե յուրաքանչյուր տրոհման դասում կա մնկից ոչ ավել բ. ֆ., որը պատկանում է M-ին։

Ցույց է տրվում, որ ք. ֆ. բազմության համար որոշված սինթեզող ալգորիթմի բարդությունը ուղիղ համեմատական կապի մեջ է այդ բազմության նկատմամբ դիզյունկտ տրոհման բարդությունից։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. И. Мальцев*, Алгоритмы и рекурсивные функции, «Наука», М., 1965. [2] *А. Н. Колмогоров*, Проблемы передачи информации, 1, 1 (1965). [3] *И. Д. Заславский*, Зап. научн. семинаров ЛОМИ АН СССР, т. 16 (1969). [4] *М. Блюм*, Сб. пер. «Проблемы математической логики», М., «Мир», 1970.