Časopis pro pěstování matematiky

Karel Čulík

Problémy z teorie minimalizace booleovských výrazů

Časopis pro pěstování matematiky, Vol. 94 (1969), No. 3, 340--353

Persistent URL: http://dml.cz/dmlcz/108603

Časopis pro pěstování matematiky, roč. 94 (1969), Praha

PROBLÉMY Z TEORIE MINIMALIZACE BOOLEOVSKÝCH VÝRAZŮ

KAREL ČULÍK, Praha *)

(Došlo 23. května 1968)

1. ÚVOD

V inženýrské praxi se úloha minimalizovat booleovský výraz řeší stále velmi často. Proto se také objevují stále nové a nové postupy řešení této úlohy a to většinou postupy inženýrské, tj. prakticky použitelné, ale ne vždy vedoucí ke skutečnému minimu. Na druhé straně se poměrně málo objevují nové výsledky, které by přineslo soustavné matematické studium jednotlivých dílčích otázek, jak je to běžné v jiných oblastech matematiky. Toto pojednání je příspěvkem k soustavnému studiu teorie minimalizace booleovských výrazů. Při tom jsou zde problémy především kladeny a jenom ve výjimečných případech jsou předložena jejich dílčí řešení. Na kladení problémů, na pokusech o jejich řešení a na jejich obměnách je předvedena celá řada heuristických metod a obratů, které se v soustavném matematickém výzkumu často používají a to v nejrozmanitějších částech matematiky a které patří k matematickému řemeslu.

Vlastním podnětem k soustavnému studiu teorie minimalizace booleovských výrazů byla potřeba sestavovat velká množství příkladů na úlohu minimalizace, ale příkladů, které by byly dostatečně representativní, tj. takové, v nichž se objeví všechna možná úskalí, protože jenom takovéto příklady jsou vhodné pro zkoušku z logiky (v 1. ročníku elektrotechnické fakulty VUT v Brně). Ukázalo se jako velice potřebné znát alespoň nějaké postačující podmínky proto, aby zvolené součiny proměnných byly minimálními implikantami nějaké booleovské funkce. A samozřejmě by bylo dobré znát i podmínky, které by byly postačující a současně nutné. Podobně by bylo velice žádoucí umět přímo ze zadání booleovské funkce rozeznat, má-li tato funkce jedinou nebo více minimálních disjunktivních (neboli součtových) forem, apod.

Všechny podobné otázky se v literatuře zařazují do výrokové logiky nebo do teorie konečných Booleových algeber. Avšak ani názvosloví ani označení není dosud jednotné. Zde je obojího použito podle [1], [2], kde lze také najít řadu dalších definic a vět, které s uvažovanou tematikou souvisí.

*) Jde o doplněnou přednášku, která byla vypracována pro katedru aplikované matematiky elektrotechnické fakulty VUT v Brně a která tam byla přednesena na výzkumném semináři ve šk. roce 1967/68

Je třeba jenom připomenout, že v logice obvyklé operace disjunkce, konjunkce a negace se zde nazývají (booleovským) součtem, součinem a inversí a značí se symboly $+$, . a $'$. Kromě toho se užívá symbolu $=$ pro rovnost dvou booleovských výrazů z hlediska jejich vyhodnocení (tj. $f = g$, kde f a g jsou booleovské výrazy, když při vyhodnocování obou výrazů pro všechna možná dosazení 0 a 1 za všechny proměnné, se vždy současně pro f i g dostane buď 1 nebo současně 0), zatímco symbolu $\equiv$ se užívá pro rovnost výrazů srovnávaných jako řetězy základních symbolů nad danou abecedou. Tedy $=$ je matematická, zatím co $\equiv$ je metamatematická rovnost. Přirozeně že se běžně užívá výrazových proměnných.

2. MINIMÁLNÍ DISJUNKTIVNÍ FORMY

Dosud každý postup pro nalezení všech minimálních disjunktivních (součtových) forem dané booleovské funkce sestával ze dvou částí. V první se najdou všechny minimální implikanty dané funkce a ve druhé se z minimálních implikant vybírají takové, že jejich součet vyjadřuje danou funkci a při tom součet délek vybraných minimálních implikant je minimální možný. Zatímco pro první část jsou známy dosti účinné algoritmy, např. Quineův nebo jeho modifikace podle McCluskeye, není pro druhou část znám žádný jiný algoritmus než probrání všech možností (samozřejmě kromě zvlášť jednoduchých případů), např. pomocí tzv. tabulky minimálních implikant. Lze ovšem udat účinný algoritmus pro nalezení všech neredukovatelných disjunktivních forem (tj. takových součtů minimálních implikant, které vyjadřují danou funkci a při tom žádnou z nich nelze vynechat, protože součet zbývajících danou funkci již nevyjadřuje). Ale při hledání minimálních disjunktivních forem je třeba probrat všechny neredukovatelné, a tato část je právě velmi neúčinná, tj. záleží skutečně v přebrání všech možností. Ovšem pro větší počet proměnných je i užití algoritmu pro první část dosti pracné a zdlouhavé.

Při sestavování representativních příkladů na druhou část předchozího postupu nezbývá nic jiného, než namátkou volit různé booleovské funkce, nalézt všechny jejich minimální implikanty a pak na tabulce zjistit, zdali jde o representativní příklad nebo nikoliv (jistě není representativní ten případ, když např. všechny minimální implikanty nebo alespoň jejich převážná většina jsou nezbytné, tj. musí být pojaty do každé neredukovatelné disjunktivní formy dané funkce), neboť pak užití tabulky je velice snadné. Kdyby bylo známo jak lze zvolit elementární součiny, aby byly množinou všech minimálních implikat nějaké booleovské funkce, daly by se uvažované příklady mnohem snadněji sestavovat. Zřejmě v tomto případě jde o následující

Problém 1. *Najděte postačující, ale co nejslabší a snadno ověřitelné podmínky (případně najděte nutné a postačující podmínky), kdy zvolená množina elementárních součinů je množinou všech minimálních implikant nějaké booleovské funkce.*

Především je zřejmé, že každá množina elementárních součinů $\{E_1, E_2, \ldots, E_n\}$, $n \geqq 1$, která je množinou všech minimálních implikant nějaké booleovské funkce, je vždy množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$. Proto v problému 1 stačí zjišťovat, zdali zvolená množina elementárních součinů $\{E_1, E_2, \ldots, E_n\}$ je množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$.

O dvou elementárních součinech E_i a E_j říkejme, že se liší v jediné inversi, když existuje taková proměnná x, že $E_i \equiv xSP$ a $E_j \equiv x'SQ$ (nebo že $E_i \equiv x'SP$ a $E_j \equiv \equiv xSQ$), kde S, P, Q jsou elementární součiny takové, že S obsahuje všechny společné proměnné obou výrazů E_i a E_j (kromě proměnné x), P obsahuje ty proměnné, které se vyskytují v E_i, ale se nevyskytují v E_j a Q obsahuje ty proměnné, které se vyskytují v E_j, ale nikoli v E_i. Při tom S i P i Q mohou být prázdné, tj. neobsahují žádnou proměnnou. Např. $yz'tw$ a $y'z'$, nebo $x'yz'w$ a $xyz'w$ se liší v jediné inversi, ale xyz' a $x'y'z'$ nikoli. Při tom nerozlišujeme součiny lišící se jen pořadím činitelů, (a podobně nerozlišujeme ani součty lišící se jen pořadím členů).

Bezprostředně z Quineova algoritmu plyne

Lemma 1. *Množina elementárních součinů $\{E_1, \ldots, E_n\}$, $n \geqq 1$, je množinou všech minimálních implikant nějaké booleovské funkce, jestliže splňuje podmínky*

(1) *E_i a E_j obsahují tytéž proměnné pro $i, j = 1, 2, \ldots, n$ a*

(2) *E_i a E_j se neliší v jediné inversi pro $i, j = 1, 2, \ldots, n$.*

Tyto postačující podmínky jsou však příliš silné. To je vidět např. z toho, že jsou postačujícími podmínkami pro to, aby množina všech minimálních implikant byla přímo množinou všech členů úplné normální disjunktivní formy dané funkce.

Druhým krajním případem podmínky typu (1) je podmínka

(3) E_i a E_j nemají žádnou proměnnou společnou pro $i \neq j$; $i, j = 1, 2, \ldots, n$.

Lemma 2. *Množina elementárních součinů $\{E_1, E_2, \ldots, E_n\}$, $n \geqq 1$, která splňuje podmínku (3), je množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$.*

Důkaz. Bez újmy na obecnosti lze předpokládat, že v žádném součinu E_i se nevyskytuje žádná inverse pro $i = 1, 2, \ldots, n$ (jinak lze všechny invertované proměnné prostě nahradit novými neinvertovanými, což plyne z (3)). Předpokládejme tedy, že $\{E_1, \ldots, E_n\}$ splňuje (3) a nechť $e_1, e_2, \ldots, e_N$ jsou všechny elementární součiny úplné normální disjunktivní formy (tj. úndf-y) booleovské funkce $\sum_{i=1}^{n} E_i$.

Indukcí dokažme, že ke každé implikantě f funkce $\sum_{i=1}^{n} E_i$ lze najít takový elementární součin E_j, že $E_j \subset f$, tj. že E_i vznikne z f vypuštěním některých proměnných. Podle definice úndf-y je zřejmé, že ke každému i, $1 \leqq i \leqq N$ existuje j, $1 \leqq j \leqq n$ takové, že $E_j \subset e_i$. Dále využijme toho, že Quineovým algoritmem lze z $e_1, e_2, \ldots, e_N$ dostat postupně všechny implikanty funkce $\sum_{i=1}^{n} E_i$ užitím známého schématu. Jsou-li tedy f_1 a f_2 libovolné dvě implikanty funkce $\sum_{i=1}^{n} E_i$, které uvedenou podmínku splňují a které se liší v jediné inversi, tj. $f_1 = gx, f_2 = gx'$, kde případně g může být prázdné (tj. $f_1 = x$, $f_2 = x'$), pak také g musí splňovat uvedenou podmínku. Kdyby totiž $E_j \not\subset g$ pro každé $j = 1, 2, \ldots, n$, pak by $E_j \not\subset gx'$ pro každé $j = 1, 2, \ldots, n$ (neboť E_j neobsahuje nikdy inversi) a to je spor. Tím je dílčí tvrzení dokázáno. Z něho však bezprostředně plyne, že $\{E_1, E_2, \ldots, E_n\}$ je množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$.

Je však zřejmé, že i podmínka (3) je příliš silná a není ani podmínkou nutnou, protože např. množina $\{xy, x'y'\}$ ji nesplňuje, ale při tom je množinou všech minimálních implikant funkce $xy + x'y'$ (což plyne i z lemmatu 1).

Když je třeba zjistit, jakým způsobem příliš silné postačující podmínky zeslabit, vždy je užitečné najít nějaké podmínky nutné a potom směrem k nim postačující podmínky zeslabovat.

S ohledem na Quineův algoritmus je přirozeným zeslabením podmínky (2) podmínka

(2*) *jestliže E_i a E_j obsahují tytéž proměnné, pak se neliší v jediné inversi pro $i, j = 1, 2, \ldots, n$.*

Lemma 3. *Množina všech minimálních implikant $\{E_1, \ldots, E_n\}$, $n \geqq 1$, booleovské funkce $\sum_{i=1}^{n} E_i$ splňuje podmínku (2*) a podmínku (4).*

(4) $$E_i \not\subset E_j \quad \text{platí pro každé} \quad i \neq j\,; \quad i, j = 1, 2, \ldots, n\,.$$

Důkaz. Nutnost podmínky (4) plyne přímo z definice minimální implikanty (kdyby totiž $E_i \subset E_j$ pro nějaké $i \neq j$, tj. kdyby $E_j \equiv E_iE$, kde E je součin obsahující alespoň jednu proměnnou, pak E_j nemůže být minimální implikantou).

Nutnost podmínky (2*) plyne přímo z Quineova algoritmu. Kdyby totiž tato podmínka neplatila, existovaly by takové minimální implikanty $E_i \not\equiv E_j$, že $E_i \equiv$ $\equiv E^*x$, $E_j \equiv E^*x'$. Potom ovšem také E^* je implikantou a tedy E_i a E_j nejsou minimální, což je spor.

Avšak ani spojení obou podmínek (2*) a (4) není postačující podmínkou pro to, aby uvažovaná množina elementárních součinů byla množinou všech minimálních implikant nějaké booleovské funkce. To plyne z následujícího příkladu: množina $\{xy, xy'z, x'yz'\}$ splňuje obě podmínky, ale booleovská funkce $xy + xy'z + x'yz' =$ $= xyz + xyz' + xy'z + x'yz'$ má za množinu všech minimálních implikant $\{xy, xz, yz'\}$.

Jiný způsob jak pokročit ve studiu množin všech minimálních implikant booleovských funkcí – často v matematice používaný s velkým úspěchem – je, pokusit se najít zákon, podle něhož se přidáváním dalších elementárních součinů k množinám všech minimálních implikant dostanou jiné množiny všech minimálních implikant booleovských funkcí. Jde tedy o to pokusit se charakterisovat útvary složitější pomocí jednodušších (např. co do počtu minimálních implikant nebo co do jejich délky). Pro to lze položit následující

Problém 2. *Nechť $\{E_1, \ldots, E_n\}$, $n \geqq 1$ je množina všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$ a nechť E_{n+1} je další elementární součin obsahující jenom takové proměnné, které se vyskytují v některém E_i, $1 \leqq i \leqq n$. Najděte nějaké nutné příp. postačující příp. nutné i postačující podmínky, kdy $\{E_1, \ldots, E_n, E_{n+1}\}$ je opět množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n+1} E_i$.*

Jestliže se upustí od požadavku, aby přidávaný elementární součin E_{n+1} neobsahoval žádné nové proměnné než ty, které se vyskytují v některém součinu E_i, kde $1 \leqq i \leqq n$, a naopak se žádá, aby obsahoval jenom nové proměnné, je odpověď snadná.

Lemma 4. *Nechť $\{E_1, \ldots, E_n\}$, $n \geqq 1$ je množina všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$ a nechť E_{n+1} je elementární součin, který neobsahuje žádnou proměnnou vyskytující se v kterémkoliv E_i, $1 \leqq i \leqq n$. Pak $\{E_1, \ldots, E_n, E_{n+1}\}$ je množina všech minimálních implikant booleovské funkce $\sum_{i=1}^{n+1} E_i$.*

Důkaz. Pro jednoduchost zase předpokládejme (bez újmy na obecnosti), že v E_{n+1} se nevyskytuje žádná inverse. Nechť $x_1, \ldots, x_k$ jsou všechny proměnné, které se vyskytují v součinech $E_1, \ldots, E_n$ a nechť $x_{k+1}, \ldots, x_h$ jsou proměnné, které se vyskytují v E_{n+1}, tj. $E_{n+1} \equiv x_{k+1} \ldots x_h$. Je-li $\sum_{i=1}^{N} e_i$ úndf-a pro $\sum_{i=1}^{n} E_i$, pak $\sum_{i=1}^{N} [e_i(x_{k+1} + x'_{k+1}) \ldots (x_h + x'_{h+1})] + [(x_1 + x'_1) \ldots (x_k + x'_k). E_{n+1}]$ po roznásobení bude úndf-ou pro $\sum_{i=1}^{n+1} E_i$. Odtud však je ihned vidět, že Quineův algoritmus se užije na obě uvedené skupiny součinů v úndf-ě nezávisle na sobě, takže skutečně $\{E_1, \ldots, E_n, E_{n+1}\}$ bude množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n+1} E_i$.

Ještě jiný způsob jak z jednodušších množin všech minimálních implikant booleovských funkcí dostat množiny složitější je násobení jednotlivých implikant navzájem. Jako užitečné se ukáže

Lemma 5. *Nechť $M = \{E_1, \ldots, E_n\}$, $n \geqq 1$ je množina elementárních součinů, nechť x je proměnná, která se nevyskytuje v žádném E_i pro $i = 1, 2, \ldots, n$ a nechť $M^* = \{xE_1, \ldots, xE_n\}$. Pak M je množinou všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$ tehdy a jen tehdy, když M^* je množinou všech minimálních implikant funkce $x(\sum_{i=1}^{n} E_i)$.*

Důkaz. Snadno se ukáže, že $\sum_{i=1}^{N} e_i$ je úndf-ou funkce $\sum_{i=1}^{n} E_i$ tehdy a jenom tehdy, když $\sum_{i=1}^{N} (xe_i)$ je úndf-ou funkce $\sum_{i=1}^{n} xE_i$. Odtud však je patrné, že Quineův algoritmus lze použít na obě úndf-y zcela paralelně, tj. že nějaký elementární součin f je implikantou funkce $\sum_{i=1}^{n} E_i$ právě tehdy, když xf je implikantou funkce $x(\sum_{i=1}^{n} E_i)$. To však zahrnuje požadované tvrzení.

Konečně další často užívaný způsob řešení úloh je specialisace na jednodušší případy. Zde půjde o množiny implikant mající malý počet prvků. V těchto jednoduchých případech se dá očekávat úplné řešení problému 1. Je zřejmé, že každý jednotlivý elementární součin je množinou všech minimálních implikant nějaké booleovské funkce (plyne to např. z lemmatu 1). Takovýto jednoduchý výsledek se dostane i pro dvouprvkové množiny minimálních implikant.

Lemma 6. *Množina elementárních součinů $\{E_1, E_2\}$ je množinou všech minimálních implikant booleovské funkce $E_1 + E_2$ tehdy a jenom tehdy, když jsou splněny podmínky* (2) *a* (4).

Důkaz. Nejdříve ukažme nutnost podmínky (2), protože nutnost podmínky (4) plyne z lemmatu 3. Dokazujeme sporem. Nechť $\{E_1, E_2\}$ je množinou všech minimálních implikant nějaké booleovské funkce, tj. také funkce $E_1 + E_2$, a nechť E_1 a E_2 nesplňují (2), tj. $E_1 \equiv SxP$ a $E_2 \equiv Sx'Q$, kde S může být popřípadě prázdné a P a Q nemají žádnou proměnnou společnou. Potom zřejmě $SxPQ$ a $Sx'PQ$ jsou elementární součiny úndf-y pro $E_1 + E_2$, takže SPQ je rovněž implikantou pro $E_1 + E_2$ a přitom $E_1 \not\subset SPQ$, $E_2 \not\subset SPQ$, z čehož plyne, že $\{E_1, E_2\}$ nemůže být množinou všech minimálních implikant pro $E_1 + E_2$.

Zbývá ukázat postačitelnost obou podmínek. Nechť tedy $\{E_1, E_2\}$ splňuje (2) a (4), tj. $E_1 \equiv S_1P$, $E_2 \equiv S_2Q$, kde S_1 a S_2 jsou elementární součiny obsahující tytéž proměnné, tj. všechny společné proměnné v E_1 a E_2 a kde P a Q zase nemají žádnou proměnnou společnou. Rozlišme dva případy:

a) Buď $S_1 \equiv S_2 \equiv S$, tj. společné části obou součinů jsou stejné. Potom však ani P ani Q nemůže být prázdné, protože platí (4), takže opakovaným užitím lemmatu 5 $\{SP, SQ\}$ a $\{P, Q\}$ současně buď jsou nebo nejsou množinami všech minimálních implikant nějaké booleovské funkce. Ale potom z lemmatu 2 plyne naše tvrzení.

b) Nebo $S_1 \not\equiv S_2$ a dokonce se S_1 a S_2 liší alespoň ve dvou inversích. Ale každý elementární součin v úndf-ě pro $E_1 + E_2$ zřejmě obsahuje buď E_1 nebo E_2 a dokažme zase indukcí, že totéž platí vůbec pro všechny implikanty funkce $E_1 + E_2$. Nechť tedy její implikanty gx a gx' uvedenou podmínku splňují. Zřejmě pak buď obě obsahují E_1 nebo obě E_2 (jinak by se nemohly lišit v jediné inversi), odkud ihned plyne, že také g musí uvedenou podmínku splňovat. Tím je současně ukázáno, že E_1 a E_2 jsou jedinými dvěma minimálními implikantami pro $E_1 + E_2$.

Obecně však podmínka (2) není nutná pro to, aby nějaká množina elementárních součinů byla množinou všech minimálních implikant nějaké booleovské funkce. To plyne z příkladu funkce $xyz + xyz' + x'yz + x'y'z$, jejíž množina všech minimálních implikant je $\{xy, yz, x'z\}$, v níž xy a $x'z$ skutečně (2) nesplňují.

3. ČÁSTEČNÉ USPOŘÁDÁNÍ IMPLIKANT

Nakonec se ještě přirozeně nabízí studovat množiny všech minimálních implikant pomocí prostředků konečných Booleových algeber nebo obecněji pomocí prostředků částečně uspořádaných množin.

Je-li $M = \{E_1, \ldots, E_n\}$, $n \geqslant 1$, množinou implikant nějaké booleovské funkce zadané svojí úndf-ou $\sum_{i=1}^{N} e_i$, pak *uzávěrem implikanty* E_i se nazývá množina $\varphi(E_i)$ definovaná podmínkou

$$(6) \qquad \varphi(E_i) = \{e_j;\ E_i \subset e_j,\ j = 1, 2, \ldots, N\}$$

a uzávěrem množiny implikant M se nazývá množina $\varphi(M) = \bigcup_{i=1}^{n} \varphi(E_i)$.

Potom vztahem inkluse mezi uzávěry je množina všech implikant dané booleovské funkce částečně uspořádána, tj. klademe $E_i \leqq E_j$, když $\varphi(E_i) \supset \varphi(E_j)$. Potom zřejmě minimální implikanty jsou minimálními prvky v tomto částečném uspořádání.

Problém 3. *Udejte nutné a postačující podmínky, kdy konečná částečně uspořádaná množina je isomorfní množině všech implikant nějaké booleovské funkce.*

4. MINIMÁLNÍ IMPLIKANTY

Při sestavování representativních příkladů na Quineův algoritmus jde o to najít takové booleovské funkce, které mají minimální implikanty různých délek. Rovněž z tohoto důvodu je žádoucí řešit problém 1, ale navíc se nabízí zodpovědět problémy týkající se různých číselných charakteristik.

Problém 4. *Jaký je maximální možný počet $\mu(n)$ minimálních implikant booleovských funkcí n proměnných? Jaký je maximální možný počet $\mu_k(n)$ minimálních implikant délky k booleovských funkcí n proměnných, kde $1 \leqq k \leqq n$? Jaké podmínky musí splňovat posloupnost nezáporných celých čísel $(m_1, m_2, \ldots, m_n)$, aby existovala booleovská funkce n proměnných, která má právě m_k minimálních implikant délky $k = 1, 2, \ldots, n$?*

Především jde o odhady zdola a shora uvažovaných čísel. Takové odhady se vždy dostanou na základě volby speciálních příkladů. Zřejmě platí $\mu(n) < 2^n$ a $\mu_k(n) <$

$< \binom{n}{k} 2^k$ pro $1 \leqq k \leqq n$. Např. pro $k = 2$ je $\mu_2(3) \geqq 6$, $\mu_2(4) \geqq 12$, když poslední odhad se opírá o následující příklad množiny minimálních implikant: $\{x_1x_2', x_1'x_2; x_2x_3', x_2'x_3; x_3x_4', x_3'x_4; x_4x_1', x_4'x_1; x_1x_3', x_1'x_3; x_2x_4', x_2'x_4\}$.

Jiným požadavkem bylo najít takové booleovské funkce, které nemají žádné nezbytné minimální implikanty a zejména takové, které mají více než jednu minimální disjunktivní formu. Proto byl položen tento problém:

Problém 5. *Udejte nutné a postačující podmínky, kdy žádná minimální implikanta booleovské funkce není nezbytná. Udejte nutné a postačující podmínky, kdy daná minimální implikanta dané booleovské funkce je její nezbytnou implikantou.*

Hned je vidět, že nutnou podmínkou pro to, aby booleovská funkce o $k \geqq 1$ proměnných neměla žádnou nezbytnou implikantu je, aby každá její minimální implikanta měla délku $< k$, tj. aby žádná minimální implikanta neobsahovala všechny proměnné.

Lemma 7. *Nechť $\{E_1, \ldots, E_n\}$ je množina všech minimálních implikant booleovské funkce $\sum_{i=1}^{n} E_i$. Pak E_i je nezbytnou implikantou tehdy a jen tehdy, když neexistují takové indexy $i_1, i_2, \ldots, i_k$ různé od i, kde $k \geqq 1$, že $\varphi(E_i) \subset \varphi_N\{E_{i_1}, \ldots, E_{i_k}\}$.*

Důkaz. Nechť $\sum_{i=1}^{N} e_i$ je úndf-a pro $\sum_{i=1}^{n} E_i$ a nechť např. E_1 je nezbytnou implikantou. Kdyby uvedená podmínky neplatila, tj. kdyby existovaly takové indexy $i_1, \ldots, i_k$, že $\varphi(E_1) \subset \varphi\{E_{i_1}, \ldots, E_{i_k}\}$ pak by ovšem tím spíše $\varphi(E_1) \subset \varphi\{E_2, \ldots, E_n\}$ a ovšem $\sum_{i=2}^{n} E_i = \sum_{i=1}^{n} E_i$. Pak vypuštěním některých minimálních implikant z množiny $\{E_2, \ldots \ldots, E_n\}$ lze dostat podmnožinu, která určuje neredukovatelnou formu neobsahující E_1 a to je spor.

Jestliže naopak E_1 není nezbytnou implikantou, pak existuje neredukovatelná forma, která neobsahuje E_1, např. $\sum_{j=1}^{k} E_{i_j}$, kde $i_j \neq 1$ pro $j = 1, 2, \ldots, k$. Pak ovšem $\sum_{j=1}^{k} E_{i_j} = \sum_{i=1}^{n} E_i = \sum_{i=1}^{N} e_i$, odkud ihned plyne, že $\varphi(E_1) \subset \varphi\{E_{i_1}, \ldots, E_{i_k}\}$, což je požadovaná podmínka.

Podmínka nalezená v lemmatu 7 je však zajímavá jen teoreticky, protože převádět minimální implikanty na odpovídající členy úndf-y je málo účinné.

Vzhledem k hledání specializovaných a účinnějších algoritmů než je Quineův je důležité řešit

Problém 6. *Udejte nutné a postačující podmínky, kdy se z množiny všech minimálních implikant dané booleovské funkce dá vybrat více než jedna minimální disjunktivní forma. Udejte nutné a postačující podmínky, kdy booleovská funkce má právě k různých minimálních disjunktivních forem.*

5. SYMETRIE BOOLEOVSKÝCH FUNKCÍ

Ve výše uvedeném příkladu s 12 minimálními implikantami jde o booleovskou funkci mající 6 minimálních disjunktivních forem. Na první pohled se vtírá domněnka, že zde budou významnou roli hrát symetrie booleovských funkcí.

Je třeba, aby nedocházelo k nedorozuměním, rozlišit dvojí pojetí funkce. Funkce n-proměnných, $n \geqq 1$, *bez pojmenování (proměnných)*, je množinou $(n + 1)$-tic, která splňuje podmínku, že neexistují dvě různé $(n + 1)$-tice, které by měly prvních n prvků stejných. Tedy lze říci, že tato funkce n-proměnných je zadána tabulkou s $(n + 1)$ sloupci, které jsou pevně uspořádané (poslední $(n + 1)$-tý sloupec je sloupec funkčních hodnot). Jestliže všech n prvních sloupců neboli prvních n míst v $(n + 1)$-ticích nějaké funkce n proměnných bez pojmenování proměnných pojmenujeme navzájem různými proměnnými $x_1, x_2, \dots, x_n$, dostaneme funkci n proměnných *s pojmenováním proměnných.*

Dvě funkce bez pojmenování jsou *stejné*, když jsou stejné množinově, tj. tabulku jedné lze převést v tabulku druhé výměnou řádků.

Naproti tomu dvě funkce s pojmenováním jsou *stejné*, když mají tytéž proměnné a když jednu lze převést v druhou vhodnou záměnou prvních n sloupců (včetně záhlaví v němž jsou proměnné) a případně i záměnou řádků.

Tedy např. v tabulkách 1. a 2. jsou dvě stejné funkce s pojmenováním,

Tab. 1

x	y	$x' + y$
0	0	1
1	0	0
0	1	1
1	1	1

Tab. 2

y	x	$x' + y$
0	0	1
1	0	1
0	1	0
1	1	1

Tab. 3

0	0	1
1	0	0
0	1	1
1	1	1

Tab. 4

0	0	1
1	0	1
0	1	0
1	1	1

ale v tabulkách 3. a 4., které vznikly z tabulek 1. a 2. prostě vymazáním proměnných, jsou dvě různé funkce bez pojmenování.

Zřejmě z jediné funkce n proměnných bez pojmenování lze dostat nekonečně mnoho různých funkcí n proměnných s pojmenováním (podle volby proměnných) a předepíšeme-li n různých proměnných, jimiž mají být sloupce pojmenovány, pak lze dostat nejvýše $n!$ různých funkcí s předepsaným pojmenováním (kolik jich bude různých záleží právě na symetriích). Ale také naopak od jedné funkce n proměnných s pojmenováním lze dostat nejvýše $n!$ různých funkcí bez pojmenování.

Funkce n proměnných bez pojmenování je *symetrická vůči i-té a j-té složce*, kde $1 \leqq i, j \leqq n$, jestliže vyměněním i-té složky j-tou a naopak v každé $(n + 1)$-tici dané funkce dostaneme funkci, která je stejná s výchozí, tj. množina $(n + 1)$-tic se nezmění. S ohledem na tabulku lze říci, že funkce je symetrická vůči i-tému a j-tému sloupci, když jejich výměnou vznikne tabulka, lišící se od původní jen výměnou řádků. Je tedy vidět, že funkce bez pojmenování, zadaná tabulkou 3 není symetrická.

Je-li funkce symetrická vůči i-tému a j-tému sloupci a také vůči j-tému a k-tému sloupci, pak zřejmě je symetrická i vůči i-tému a k-tému sloupci. Tedy binární relace symetričnosti vůči dvojicím sloupců je ekvivalencí a proto se množina všech sloupců (čili množina přirozených čísel $1, 2, \ldots, n$, která udávají pořadí sloupců v tabulce v uspořádání zleva doprava) jednoznačně rozloží na neprázdné a navzájem disjunktní podmnožiny navzájem symetrických sloupců. Nechť T je množina všech sloupců (čili přirozených čísel $1, 2, \ldots, n$) a nechť $T_1, T_2, \ldots, T_t$ jsou její podmnožiny, patřící uvažovanému rozkladu, které lze nazvat *komponentami symetrie dané funkce*. Z předchozích definic je hned vidět, že platí

Lemma 8. *Jsou-li $T_1, \ldots, T_t$ všechny komponenty symetrie dané funkce bez pojmenování, pak tato funkce je symetrická vůči i-té a j-té složce tehdy, když existuje index h, $1 \leqq h \leqq t$ takový, že $i \in T_h$ a $j \in T_h$.*

Je-li π libovolná permutace množiny $T = T_1 \cup \ldots \cup T_t$, pak výměnou i-tého sloupce za $\pi(i)$-tý pro každé $i \in T$ se daná funkce nezmění (tj. vzniklá tabulka se liší od dané jen pořadím řádků) tehdy a jen tehdy, když $\pi = \pi_1\pi_2 \ldots \pi_t$, kde π_i je nějaká cyklická permutace na komponentě symetrie T_i dané funkce pro $i = 1, 2, \ldots, t$.

Odtud je patrno, že množina komponent symetrie dané funkce je zobecněním pojmu symetrie vůči dvěma složkám či sloupcům. Uvažované permutace složek či sloupců lze nazvat *automorfismy symetrie* dané funkce. Je potom zřejmé, že množina všech komponent symetrie dané funkce je systémem transitivity grupy všech automorfismů, která je zřejmě přímým součinem právě symetrických permutačních grup definovaných na jednotlivých komponentách symetrie.

Je ihned zřejmé, že přejdeme-li od dané funkce bez pojmenování k nějaké jí odpovídající (tj. z ní vzniklé) funkci s pojmenováním, že všechny předešlé pojmy a úvahy lze opakovat i v tomto případě, takže lze hovořit o symetrii vůči proměnným x a y, dále, že relace symetričnosti definované na množině všech proměnných P je zase ekvivalencí a konečně, že podmnožiny P_i příslušného rozkladu lze nazvat komponentami symetrie dané funkce. Jestliže víme např., že i-tý sloupec byl pojmenován proměnnou x_i pro $i = 1, 2, \ldots, n$, pak mezi T_j a P_j je určeno jedno-jednoznačné přiřazení a zřejmě funkce s pojmenováním je symetrická vůči proměnným x_i a x_j právě tehdy, když po výměně samotných sloupců pojmenovaných x_i a x_j v nějaké tabulce (tj. bez výměny jejich záhlaví x_i a x_j) dostaneme tabulky téže funkce s pojmenováním.

Ve zvoleném případě proměnné $x_1, \ldots, x_n$ jsou očíslovány a tedy dovolují zvolit jedno význačné uspořádání, totiž podle velikosti indexů. V tomto případě se obvykle mezi všemi možnými tabulka uvažované funkce s pojmenováním volí jedna význačná, totiž ta, jejíž i-tý sloupec je právě pojmenován proměnnou x_i pro $i = 1, 2, \ldots, n$. Je tedy zřejmé, že v tomto případě se dá najít přirozené jedno-jednoznačné přiřazení mezi funkcemi s pojmenovanými proměnnými $x_1, \ldots, x_n$ a odpovídajícími funkcemi bez pojmenování.

Avšak funkce s pojmenovanými proměnnými byly zavedeny proto, že se zadávají nikoliv tabulkou, ale nějakým funkčním výrazem, který záleží na zvolených základních funkcích, z nichž ostatní skládáme. Zde jde přirozeně o booleovské funkce a tedy o booleovské výrazy. Je totiž ihned zřejmé, že proměnnými booleovského výrazu lze nazvat všechny ty proměnné, které se v něm vyskytují. Pak ovšem je patrno, že existuje přirozené přiřazení mezi booleovskými výrazy a booleovskými funkcemi s pojmenovanými proměnnými, totiž vyhodnocením každého booleovského výrazu (obsahujícím nějaké proměnné) dostaneme jedinou booleovskou funkci se stejnými proměnnými jako má daný výraz (to je případ výrazu $x' + y$ v tab. 1 a 2), ale obecně, tj. někdy, dostaneme více než jednu booleovskou funkci bez pojmenovaných proměnných (to je případ dvou různých funkcí v tabulce 3 a 4).

Konečně je třeba si uvědomit, že zjišťovat rozmanité symetrie dané booleovské funkce, tj. všechny možné dvojice sloupců, vůči nimž je daná funkce symetrická, je velice zdlouhavé. Když k tomu připojíme, že navíc velmi často jsou booleovské funkce zadány booleovskými výrazy a tedy při zjišťování symetrií je především třeba sestavit jejich tabulky, pak je žádoucí najít nějaké jiné podmínky (než definiční), které se týkají přímo booleovských výrazů a které by bylo možné prověřovat snadněji. Potíž zde může být v tom, že každá booleovská funkce s pojmenovanými proměnnými může být vyjádřena nekonečně mnoha různými booleovskými výrazy a my chceme o jejich symetriích rozhodnout podle kreréhokoliv z nich. Proto je především třeba najít nějaké takové vlastnosti booleovských výrazů, které se nemění při přechodu k jiným výrazům, které však vyjadřují tutéž funkci.

Lemma 9. *Nechť π je libovolná permutace booleovských proměnných $(x_1, \ldots, x_n)$ a nechť f^* příp. g^* je booleovský výraz, který vznikne o booleovského výrazu f příp. g tak, že místo každého výskytu proměnné x_j se dosadí $\pi(x_j)$ pro $j = 1, \ldots, n$. Jsou-li $x_1, \ldots, x_n$ společné proměnné výrazů f a g a je-li $f = g$, pak $f^* = g^*$.*

Důkaz. Bez újmy na obecnosti předpokládáme, že mezi proměnnými $x_1, \ldots, x_n$ se vyskytují všechny proměnné vyskytující se v f nebo v g (v opačném případě chybějící proměnné přidáme k proměnným $x_1, \ldots, x_n$ a π rozšíříme tak, aby každou přidanou proměnnou převáděla v sebe).

Jestliže ve výrazu f místo každého výskytu proměnné x_j dosadíme booleovskou konstantu i_j pro každé $j = 1, \ldots, n$, pak dostaneme týž booleovský výraz (bez proměnných), který dostaneme z výrazu f^* jestliže v něm místo každého výskytu proměnné $\pi(x_j)$ dosadíme booleovskou konstantu i_j pro $j = 1, \ldots, n$ (protože f^* vznikne z f dosazením $\pi(x_j)$ tam, kde bylo x_j pro $j = 1, \ldots, n$). Po uvedeném dosazení vyjadřují f i f^* touž booleovskou konstantu. Avšak totéž platí i pro výrazy g a g^*, v nichž dosazujeme i_j za x_j a za $\pi(x_j)$ pro $j = 1, \ldots, n$. Nyní však je zřejmé, že z $f = g$ plyne $f^* = g^*$.

Věta 1. *Booleovská funkce s pojmenováním je symetrická vůči proměnným x a y tehdy a jen tehdy, když pro nějaký booleovský výraz f, který tuto funkci vyjadřuje, platí toto: je-li f^* booleovský výraz vzniklý z booleovského výrazu f tím, že každý výskyt proměnné x příp. y v f se nahradí výskytem proměnné y příp. x, pak $f^* = f$, tj. f^* i f vyjadřují tutéž booleovskou funkci.*

Důkaz. Nechť pro nějaký booleovský výraz f, který vyjadřuje danou booleovskou funkci s pojmenováním, platí $f^* = f$. Pak stačí si uvědomit, že z libovolné tabulky s pojmenovanými sloupci, která vznikla vyhodnocením výrazu f (a která je tedy vlastně danou funkcí), dostaneme — výměnou jejích sloupců, pojmenovaných proměnnými x a y — tabulku, která vznikne vyhodnocením výrazu f^*. To ovšem znamená, že daná funkce je symetrická vůči proměnným x a y. A podle lemmatu 9 toto rozhodnutí o symetrii nezávisí na volbě výrazu f, neboť pro libovolný jiný výraz g, který vyjadřuje danou funkci, platí $f = g$, odkud plyne, podle lemmatu 9, $f^* = g^*$. Avšak pomocí $f^* = f$, odtud plyne i $g^* = g$, takže předchozí úvaha povede k rozhodnutí o symetričnosti i při volbě výrazu g.

Nechť naopak daná booleovská funkce s pojmenováním je symetrická vůči proměnným x a y, tj. nechť pro (nějakou) její tabulku s pojmenovaným záhlavím platí, že výměnou sloupců x a y (bez výměny samotného záhlaví, tj. proměnných) vznikne tabulka, která se od původní liší jen pořadím řádků. Avšak daná tabulka je tabulkou (nějakou), která vznikne při vyhodnocení libovolného výrazu f, který danou funkci vyjadřuje, a dále nová tabulka je zřejmě (nějakou) tabulkou, vzniklou vyhodnocením výrazu f^*. To znamená ovšem $f^* = f$.

Užitečnost věty 1 je v tom, že dovoluje dokazovat obvyklými prostředky booleovy algebry rovnost nebo nerovnost mezi výrazy f a f^*, místo aby se přímo pracovalo s příslušnými tabulkami.

Problém 7. *Jaký typ symetrie booleovských funkcí je postačující podmínkou pro to, aby tyto funkce měly více než jednu minimální disjunktivní formu?*

Že v obecném případě jakákoliv symetrie není nutnou podmínkou pro to, aby booleovská funkce měla více než jednu minimální disjunktivní formu, plyne z následujícího příkladu. Booleovská funkce $xz' + yz' + xyz' + xy'w$ má dvě minimální disjunktivní formy: kromě již uvedené je to druhá $xz' + yz' + xyz' + xz'w$. Obě se od sebe liší jen v posledních minimálních implikantách $xy'w$ a $xz'w$, ale daná funkce patrně není symetrická vůči y a z a patrně ani vůči jiným dvojicím proměnných.

Naproti tomu např. booleovská funkce daná výrazem $xyz' + xyz' + xy'z +$

$+ xyz'' + xy'z' + xy''z$, která je zřejmě symetrická vůči každým dvěma proměnným, má množinu všech implikant $\{xz', xy', yz', xy', yz', xz'\}$ a má právě dvě minimální disjunktivní formy $xy' + yz' + zx'$ a $xy' + yz' + zx'$.

Literatura

[1] *K. Čulík, V. Doležal, M. Fiedler:* Kombinatorická analýza v praxi, SNTL, Praha 1967.

[2] *K. Čulík, M. Skalická, I. Váňová:* Logika I, Učební texty vysokých škol, SNTL 1968.

Adresa autora: Praha 1, Žitná 25 (Matematický ústav ČSAV).

Summary

THE PROBLEMS IN MINIMALIZATION THEORY OF BOOLEAN EXPRESSIONS

Karel Čulik, Praha*)

There are proved several partial results and mentioned the particular motivations concerning the following problems:

Problem 1. Find easy verifyable, as weak as possible, sufficient conditions when the given set of elementary conjunctions is a set of all prime implicants of a boolean function with given variables!

Problem 2. Let $\{E_1, \ldots, E_r\}$, $p \geqq 1$, be the set of all prime implicants of a boolean function with variables $x_1, \ldots, x_n$, $n \geqq 1$ a let E_{p+1} is an elementary conjunction over the same variables. Find the necessary or sufficient (or both necessary and sufficient) conditions when $\{E_1, \ldots, E_p, E_{p+1}\}$ is the set of all prime implicants of a boolean function again!

Problem 3. Find the necessary and sufficient conditions when a partial ordered set is isomorphic to the set of all implicants of a boolean function which is partially ordered by the requirement „to be part of"!

Problem 4. Determine the maximal number $\mu(n)$ [or $\mu_K(n)$] of prime implicants [having the length k] of boolean functions with n variables [$1 \leqq k \leqq n$]!

*) This paper was supported by the Faculty of Electroengineering of the Technical university in Brno and was prepared and read in the research seminar at its department of applied mathematics in 1967/68.

What are the necessary and sufficient conditions when the given sequence of integers $(m_1, \ldots, m_n)$ satisfies the following requirement: there exists a boolean function with n variables having exactely m_k prime implicants of the length k for $k = 1, \ldots, n$?

Problem 5. Find the necessary and sufficient conditions when the given prime implicant of a boolean function belongs to each minimal disjunctive form of it! Such a prime implicant is called necessary. Determine the necessary and sufficient conditions when the given boolean function does not have any necessary prime implicant!

Problem 6. Find the necessary and sufficient conditions when the given boolean function has more than one minimal disjuntive form [or has exactely $k \geqq 1$ different minimal disjunctive forms]!

Problem 7. What types of symmetry of a boolean function are and what are not sufficient condition for the existence of more than one minimal disjunctive form of that function?