Полуалгебраичные системы доказательств

Все системы доказательств оперируют с многочленами. Формула в кнф записыается так: Для каждого клоза, содержащего переменные x_i и отрицания y_i, берется уравнение $(1-x_1)*(1-x_2)*\cdots*(1-x_n)*y_1*y_2*\cdots*y_m=0$, так как переменные еа самом деле 0 или 1, fr;t добавляются уравнения $x*x=x$ для всех переменных. Мы будем не доказывать наличие выполняющего набора, а добавлять ее отрицание в систему и доказывать противоречивость системы.

Системы доказательств

Nullstellensatz(NS) - Изначально у нас есть система уравнений $f_i=0$, доказательство противоречивости -набор $g_i : \sum f_i*g_i=1$, такие по тореме Гильберта о нулях существуют над алг. замкнутым полем.

Polynomial calculus (PC) - вывод док-ва в Nullstellensatz: из уравнения p=0,q=0 выводится p+q=0, из p=0 выводится pq=0. Доказательство противоречивости - вывод $1=0$.

Pozitivestellensatz(PSZ) - многочлены над R, есть система уравнений $f_i=0$, доказательство противоречивости - набор $g_i, h_i : g_i : \sum f_i*g_i=1+\sum h_i^2$.

Positivestellensatz calculus (PSZC) - вывод док-ва в Positivestellennsatz, правила вывода те же, что и в PC, а док-во противоречивости - набор многочленов h_i и вывод $0=+\sum h_i^2$ из правил вывода.

Lovasz-Schreier calculus (LS) - манипулируем не с равенствами, а с неравенствами, из $f_1\geq 0, f_2\geq 0,\ldots,f_n\geq 0$ выводится $\sum a_i f_i\geq 0$, где $a_i\geq 0$ - константы. Также из $f\geq 0$следует $fx\geq 0, f(1-x)\geq 0$ для переменной x. Аксиомы - $x^2-x\geq 0, x-x^2\geq 0$ для всех переменных x. Вывод противоречия - вывод $-1\geq 0$.

LS_+ - то же, но еще есть аксиома $l^2\geq 0$ для любого полинома l.

Булева степень многочлена - степень многочлена, взятого по модулю $x_i^2-x_i$ для всех переменных в нем. Булева степень доказательства - максимальная из булевых степеней многочлена в процессе.

Мы доказываем несуществование решения задачи о рюкзаке (доказываем несуществование x_i, таких что $f=x_1+x_2+\ldots+x_n=m$)) при нецелом m, то есть добавляем f в систему и доказываем противоречивость. Пусть $A(m)$ - ступенчатая функция, равная 0 вне $[0,n]$, $2k+4$ на $[k,k+1]$ и $[n-k-1,n-k]$.

Th: Булева степень любого док-ва неразрешимости задачи о рюкзаке в PC не менее $\frac{(n-1)}{2}$, в PSCZ - не менее $min(\frac{n-1}{2},A(m))$.

Th: Размер любого доказательства неразрешимости задачи о рюкзаке при $m=\frac{2n+1}{4}$ в NS и PSZ экспоненциален.

Статические доказательства

NS - статическая версия PC, PSZ - статическая версия PSZC.

Static LS: - пусть есть система неравенств $s_i\geq 0$. Доказательство ее противоречивости - набор многочленов $w_{i,j}$, каждый из которых - произведение мономов $x_i,(1-x_i)$ и констант $a_{i,j}\geq 0$, такой что $\sum s_i\sum a_{i,j}w_{i,j}=-1$.

Static LS_+: - пусть есть система неравенств $s_i\geq 0$. Доказательство ее противоречивости - набор многочленов $w_{i,j}$, каждый из которых - произведение мономов $x_i,(1-x_i)$ или квадрат другого многочлена и констант $a_{i,j}\geq 0$, такой что $\sum s_i\sum a_{i,j}w_{i,j}=-1$.

Th: при $m=\frac{2*n+1}{4}$ размер любого док-ва рюкзака в Static LS, Static LS_+ экспоненциален от n.