

Skúmame dokázateľnosť tvrdení z teórie zložitosti v obmedzenej aritmetike. Za istých zložitostných predpokladov ukážeme, že teórie so slabšími dosvedčovacími vlastnosťami než  $S^1_2$  nemôžu dokázať spodné odhady veľkosti  $n^k$  na booleovské obvody pre SAT vyjadrené formulou  $LB(SAT, n^k)$ . Špeciálne, prvorádová teória pravdivých univerzálnych tvrdení v jazyku obsahujúcom symboly pre všetky uniformné  $NC^1$  algoritmy nedokazuje  $LB(SAT, n^{4kc})$  pre  $k \geq 1, c \geq 2$  predpokladajúc existenciu funkcie  $f \in SIZE(n^k)$ , ktorá nie je aproximovateľná formulami  $F_n$  subexponenciálnej veľkosti  $2^{O(n^{1/c})}$  so subexponenciálnou výhodou:  $P_{x \in \{0,1\}^n} [F_n(x) = f(x)] \geq 1/2 + 1/2^{O(n^{1/c})}$ . Bezpodmienečne, teória  $V^0$  nedokazuje kvazipolynomiálne spodné odhady na booleovské obvody pre SAT. Čo sa týka horných odhadov, dokážeme PCP vetu v Cookovej teórii  $PV_1$ . To zahŕňa formalizáciu  $(n, d, \lambda)$ -grafov v  $PV_1$ . Ako dôsledok dostaneme polynomiálne krátke Extended Frege dôkazy tautológií vyjadrujúcih PCP vetu.