This paper consists of two parts both of which attempt to provide tautologies which might be hard for a propositional proof system P. Finding hard tautologies is of interest as a possible approach to the NP versus $\mathsf{co}-\mathsf{NP}$ problem. The first part of the paper continues the study of the $\tau(g)_b(x)$ tautologies begun in Krajíček [1]. These tautologies express that $b \in \{0,1\}^m$ is not the output of $g(x)$ for a function $g : \{0,1\}^n \longrightarrow \{0,1\}^m$ with $m > n$ computed by a polynomial sized circuit family. In the earlier Krajíček paper, $\tau(g)_b(x)$ tautologies, where g computes a certain pseudo-random number generator, were put forward as candidate hard tautologies for propositional proof systems like extended Frege. Another choice of g suggested in this earlier paper was the function tt which takes as input a circuit C of size at most $2^{k/2}$ with k inputs and outputs the truth table for C. The first part of the present paper gives two example tautologies, which if they had short proofs, would imply the $\tau(g)_b(x)$ tautologies have short proofs. The second part of the present paper gives a family of tautologies which would be hard for P if a certain condition about an implicit proof system is met.

The first tautologies presented in the first part of the paper are based on tournaments. Razborov [3] gives a $m^{O(1)}$ sized circuit family $\{D_m\}$ with $2m$ inputs which computes the edge relation of a tournament on $\{0,1\}^m$ vertices that has no dominating set of size n. If C_n computes tt for n bit inputs, then one can define $E_n(x,y)$ as $D_n(C_n(x), C_n(y))$ if $x \neq y$, as 1 if $x = y$, and 0 otherwise. The graph with this edge relation is a tournament on the vertices consisting of strings in $\{0,1\}^n$. From the theory of tournaments, it has a dominating set of size n; however, given the properties of D_m and C_n this dominating set is presumably hard to find. Let $A_n \subseteq \{0,1\}^n$ be such a dominating set. The hard tautologies express $\bigvee_{a \in A_n} x = a \vee E_n(a,x)$. It is shown that if there is any g as in the first paragraph which is exponentially iterable for a proof system P, then these hard tautologies require super-polynomial sized P-proofs. Exponentially iterable means any disjunction of the form $\tau(g)_{B_1}(q^1) \vee \tau(g)_{B_1}(q^1,q^2) \vee \cdots \vee \tau(g)_{B_k}(q^1,\ldots,q^k)$ requires 2^{n^ϵ} sized P-proofs. Here q^j are m-tuples that the input variables to the given disjunct must be among, and the B_k are m-output circuits, each output computed as either a variable of some q^j for $j < k$ or computed as a constant. In particular B_1 has no variables.

The second tautologies presented in the first part of the paper are based on viewing $\{0,1\}^m$ as a vector space with a coordinate-wise addition $\oplus_m$ and an inner product $\langle , \rangle$. Define relations $R'_n(x,y,z)$ as $C_n(x) \oplus C_n(z)$ and $S'(x,y)$ as $\langle x,y \rangle = 1$. Let $x \sim y$ if and only if $C_n(x) = C_n(y)$ and let R_n

and S_n be $R'_n/\sim$ and $S'_n/\sim$ respectively. The tautologies considered express that there is a sequence of n-tuples $u_1, \ldots, u_n$ such that for any n-tuples x and y either $\neg R_n(u_1/\sim, u_2/\sim, y/\sim)$ or for some u_i, $S_n(u_i/\sim, x/\sim)$. The result is, again, if there is any g as above which is exponentially iterable for a proof system P, then these tautologies require super-polynomial sized proofs.

The second part of the paper makes use of the notion of implicit proof system from Krajíček [2]. Given two proof systems P and Q with P containing resolution, one can define an implicit system $[P, Q]$ whose proofs consist of pairs (α, β) where $\beta(i, j)$ is a circuit that is supposed to check if j encodes the ith instantaneous description of a computation of a polynomial time machine checking a Q-proof of some tautology τ, and α is a P proof of the fact that all the $\beta(i, j)$'s satisfy the local conditions of a valid computation of a Q-proof on some input. Krajíček [2] shows $[EF, EF]$ proofs system simulate the $\forall\Pi^b_1$-consequences of the bounded arithmetic theory V^1_2. Here EF is the extended Frege proof system. In the present paper this is used to show that there are $s^{O(1)}$-sized $[EF, EF]$-proofs of tautologies based on search problems connected to the weak pigeonhole principle (WPHP) and to Ramsey theory. The former search problem asks given a size s circuit D computing a map from m to n where $m > n$, to find two different elements which map to the same point; the latter asks to find a homogeneous set of size in m in a graph on $\{0, 1\}^{2m}$ whose edge relation is computed by a size s circuit D. On the way to showing the main result of the second part of the paper, it is shown that the search problem WPHP, finding a collision in a family of p-time hash functions, and decoding RSA can all be $\mathsf{P/poly}$ many-one reduced to the RAM search problem. The main result of the second part of the paper is that if there is an implicit proof system $[P, Q]$ such that the tautology based on RAM has $n^{O(1)}$ sized proofs for circuits of size s between n and $n^{O(1)}$, yet the tautology based on WPHP has $n^{\omega(1)}$ sized proofs for circuits of size t a different function of size between n and $n^{O(1)}$; then a tautology asserting no homogeneous set of size $2n$ exists in a graph given whose edges are computed by a particular circuit from Razborov [3] requires super-polynomial sized P-proofs. Here it is require that P contains resolution and Q contains tree-like resolution.

Both parts of the paper are self-contained and interesting, and the paper as a whole is remarkably succinct given the amount of material covered.

References

[1] J. Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *Journal of Symbolic Logic.* Vol. 69. Issue 1. 2004. pp. 265–286.

[2] J. Krajíček. Implicit proofs. *Journal of Symbolic Logic.* Vol. 69. Issue 2. 2004. pp. 387–397.

[3] A. A. Razborov. Formulas of bounded depth in the basis (&, $\oplus$) and some combinatorial problems. *Voprosy Kibernetiki.* Vol. 234. 1988. pp. 149–166.