This paper proposes tautologies which might be hard for proof systems such as extended Frege (EF). It then attempts to justify this conjectured hardness. Frege systems are the kinds of propositional proof systems one might see in an introductory logic class where one has a finite number of axiom schemes and modus ponens. An Extended Frege proof system extends such a system with the ability to abbreviate formulas by news atoms. The study of propositional proof systems is motivated by NP vs. coNP problem.

The hard formulas the paper considers are instances of τ-formulas. Let g be a function from n to m bits where $m > n$ that is computed by a circuit family $\{C\_n\}$ of size s, and let $b \in \{0,1\}^m$ be outside g's range. Then $\tau(C)_b$ is a DNF formula expressing if $C(x) = y$, then b and y differ on some bit value. The paper proposes that such a τ-formula, where a modified Nisan Widgerson pseudorandom number generator [2] is used for g, will be hard. To define a what a Nisan Widgerson generator is, let A be an n by m, 0-1 valued matrix which has at most ℓ ones in any row. If f is a boolean function from strings of length less than ℓ, then the generator, $NW_{A,f}$, is the function which on x, an n-bit number, outputs y, an m-bit number, where the ith bit of y is $f(x_{j_1}, \ldots, x_{j_u}) = 1$. Here j_k are the 1 columns of the ith row of A in order, and x_m is the mth bit of x.

To motivate why τ tautologies might by hard when such Nisan Widgerson generators are used the paper proves three results: The first result concerns an arbitrary propositional proof system P and and a function g as above computed by a polynomial sized circuit family, $\{C_n\}$. The papers shows for any polynomial p, that if $\epsilon(m)$, for $m > 0$, is always strictly less than a half and if any $NP/poly$ set A in the complement of g's range has fewer than $\epsilon(m) \cdot 2^m$ strings of length m, then with probability greater than $1/2 - \epsilon(m)$, $\tau(C_n)_b$ require proofs of size greater than p. Thus, this result gives a sufficient condition where a τ-formula might be hard. The paper defines two notions, pseudo-surjectivety and iterability – with the former being stronger, which very roughly say that after 'composing' g with itself multiple times, it is still hard to prove there is some string not in the range of the resulting function. The paper proves a number of closure conditions for these two notions and connects the existence of pseudo-surjective and iterable g to the existence of truth table functions which are pseudo-surjective or iterable. For the second main result, it is shown that any proof system which can simulate EF and does not admit a pseudo-surjective function must be able to simulate the proof system WF proposed by Jeřábek [1]. This system is known to be able to prove propositional translations of statements from Buss' theory

S_2^1 together with the weak pigeonhole principle for p-time function. As S_2^1 is conjectured not to be able to prove the weak pigeonhole principle on its own, this indicates iterations of τ tautologies for a well chosen g might be harder than EF. Finally, with regard to τ-formulas based on Nisan Widgerson generators, it is shown that at least in the case of resolution refutations there is an iteration protocol for a Nisan Widgerson generator which is $2^{n^{1-\delta}}$ hard. This paper is very interesting and seems like a promising area for future research.

References

[1] E. Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Annals of Pure and Applied Logic.* Vol. 129 Issue. 1–3. pp. 1–37. 2004.

[2] N. Nisan and A. Widgerson. Hardness versus Randomness. *Journal of Computer and System Science.* Vol. 49. pp. 149-167. 1994.