This paper proposes a general approach to finding lower bounds on the sizes of proofs in propositional proof systems based on pseudo-random number generators: Basically, one should look at tautologies which express that a given bit vector is not in the range of an appropriately chosen pseudo-random number generator. A similar approach has also been proposed by Krajíček [1]. Some interesting examples of previously obtained lower bound results for Tseitin tautologies, natural proofs, and feasible interpolation are shown to fit within this paradigm. Using this approach the paper proves lower bounds for several propositional proof systems using tautologies based on matrices which have an expansion property. The paper uses three encoding schemes to express its tautologies: a functional encoding scheme, a circuit encoding scheme, and a linear encoding scheme. Lower bounds are obtained for resolution, the polynomial calculus, and the polynomial calculus with resolution. The paper is very clear and concludes with some pointers into the literature on the topic after this paper was initially written.

References

[1] J. Krajíček. On the weak pigeonhole principle. Fundamenta Mathematica. Vol. 170. 2001. pp. 123–140.