# Resolution with Counting: Different Moduli and Tree-Like Lower Bounds

Fedor Part[1] and Iddo Tzameret[2]

[1] Department of Computer Science Royal Holloway, University of London
Fjodor.Part.2012@live.rhul.ac.uk
[2] Department of Computer Science Royal Holloway, University of London
Iddo.Tzameret@rhul.ac.uk

We study the complexity of resolution extended with the ability to count over different characteristics and rings. These systems capture integer and moduli counting, and in particular admit short tree-like refutations for insolvable sets of linear equations. For this purpose, we consider the system $\mathrm{Res}(\mathrm{lin}_R)$, as introduced in [5], in which proof-lines are disjunction of linear equations over a ring $R$.[3] Extending the work of Itsykson and Sokolov [3] we obtain new lower bounds and separations, as follows:

**Finite fields:**

1. Exponential-size lower bounds for tree-like $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}_p})$ refutations of Tseitin mod $q$ formulas, for every pair of distinct primes $p, q$. As a corollary we obtain an exponential-size separation between tree-like $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}_p})$ and tree-like $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}_q})$.
2. Exponential-size lower bounds for tree-like $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}_p})$ refutations of random $k$-CNF formulas, for every prime $p$ and constant $k$.
3. Exponential-size lower bounds for tree-like $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}})$ refutations of the pigeonhole principle, for *every* field $\mathbb{F}$.

All the above hard instances are encoded as CNF formulas. The lower bounds are proved using extensions and modifications of the Prover-Delayer game technique [4, 3] and size-width relations [2].

**Characteristic zero fields:** Separation of tree-like $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}})$ and (dag-like) $\mathrm{Res}(\mathrm{lin}_{\mathbb{F}})$, for characteristic zero fields $\mathbb{F}$. The separating instances are the pigeonhole principle and the Subset Sum principle. The latter is the formula $\alpha_1 x_1 + \ldots + \alpha_n x_n = \beta$, for some $\beta$ not in the image of the linear form. The lower bound for the Subset Sum principle employs the notion of *immunity* from Alekhnovich and Razborov [1].

## References

1. Alekhnovich, M., Razborov, A.A.: Lower bounds for polynomial calculus: non-binomial case. In: Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), pp. 190–199. IEEE Computer Soc., Los Alamitos, CA (2001)

[3] We focus on the case where the variables are Boolean, i.e., we add the Boolean axioms $(x_i = 0) \vee (x_i = 1)$, for all variables $x_i$.

2. Ben-Sasson, E., Wigderson, A.: Short proofs are narrow—resolution made simple. J. ACM **48**(2), 149–169 (2001)
3. Itsykson, D., Sokolov, D.: Lower bounds for splittings by linear combinations. In: Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part II. pp. 372–383 (2014). https://doi.org/10.1007/978-3-662-44465-8_32, https://doi.org/10.1007/978-3-662-44465-8_32
4. Pudlák, P., Impagliazzo, R.: A lower bound for DLL algorithms for $k$-sat (preliminary version). In: Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, January 9-11, 2000, San Francisco, CA, USA. pp. 128–136 (2000), http://dl.acm.org/citation.cfm?id=338219.338244
5. Raz, R., Tzameret, I.: Resolution over linear equations and multilinear proofs. Ann. Pure Appl. Logic **155**(3), 194–224 (2008). https://doi.org/10.1016/j.apal.2008.04.001, http://dx.doi.org/10.1016/j.apal.2008.04.001