Opinion on "Multiplication in a finite field of characteristic 2 and XOR-metrics"

Recently, Kölsch resolved a conjecture on characterization of elements whose multiplication matrix can be implemented with just two XOR-operations [Köl19]. In this paper, Kölsh also shows the *sequential* s-XOR-count is not in general lower than *direct* d-XOR count disproving a previous conjecture. He gave a 7×7 matrix with coefficients from $\mathbb{F}_2$.

In the reviewed work, Carulkov takes on the natural question whether this is the smallest counter example. Indeed he proves that (Theorem 2.6) there are examples when $n = 6$ and also that (Theorem 2.7) $n = 6$ is the smallest case. He also gives a construction for such matrices for every $n \geq 6$. The author uses very good techniques to prove these results.

I can safely say the submitted thesis deserves the best grade.

I should mention that the work would have been a much better read if the author had included a more detailed introduction on the subject. However this criticism is only minor, and I think the work is very good and certainly deserves the best grade.

A few editorial comments:

- p.2 emerge -: emergence
- (overall) definition 1, theorem 5, etc. should be -: Definition 1, Theorem 5, etc.
- (overall) In an academic text one should avoid using colloquial shortened forms such as *we'll, can't, won't*.
- (overall) "Proof" instead of "Dukaz".
- p.7 "in a cycle normal form" -: "in cycle normal form".
- p.10 "switch the the" :- delete "the".

Faruk Göloğlu
Prague, June 22nd, 2020