RESPONSE TO THE REFEREE'S COMMENTS ABOUT "GOPPA–LIKE AG CODES FROM $C_{a,b}$ CURVES AND THEIR BEHAVIOUR UNDER SQUARING THEIR DUAL"

SABIRA EL KHALFAOUI, MATHIEU LHOTEL AND JADE NARDI

We took in account all the comments of the referees and we modified the manuscript accordingly. To help the referees to better navigate in this answer and the revised version, we have listed all the comments below, followed by our answer.

Common comments

First review's comment

The main result of this paper is Theorem 3.8 on the upper bound of the dimension of codes. Some problems of this paper are :

- There are many symbols. Please give a clear description of symbols, which can make the paper more readable.
- Please give more clear comparisons and show the clear advantages of this paper. Add some some results of [NEK21] in Table 1 to give a clear comparison. Add some examples in Section 2 to make a comparison with results in Section 3.

Hence, I suggest a revision. Some more comments are listed:

- Page 1. Section Introduction. Line 16. "The scheme ... have";
- Page 1. Subfield subcodes of AG codes. Line -7. Note the symbols of codes and curve. Check the use of C and C;
- Page 2. It is better to give a clear description of the advantages of the upper bound of the dimension of codes.
- Page 2. Line 14 in Contributions of this paper. "performing ... enable ...";
- Page 3. Line -13. "a [n, k]". Many similar errors in the paper;
- Page 5. Please check the use of $Tr(C)^2$ and C^{q^i} . It seems that $Tr(C)^2$ means $Tr(C^2)$. Many similar problems in the paper. Please give a description of Cqi .
- Page 6. Note that $\deg G = s$. There are many symbols in the paper. Please give a clear description.
- Page 7. Line 1. "the product ... belong ...";
- Page 8. Line 2 in Remark 2.2. "Theorem 1.4 and 1.6"; Line 1 in Section 2.1.1. "define"; Line 5 in Section 2.1.1. "an correcting ";
- Page 11. It is better to give some examples at the end of Section 2;
- Page 13. Line -9. "there is a few cases ...";
- Page 15. Corollary 3.7. Line 3. A (was omitted. Please check the rest of the paper;
- Page 18. Check the format of references. Update Reference [MT21].

Second review's comment

- Page 1, line 6: "The security of McEliece cryptosystem." This should be something like "The security of the McEliece cryptosystem". Similar minor grammatical issues occur elsewhere in the paper as well. I recommend a careful check of the entire paper.

- Page 1, line 13: "Høhold and Pellikaan" should be "Høholdt and Pellikaan".
- Page 2, line 1: "$C_L(X, P, D + (g))$". Elsewhere the P is in mathcal font, but not here.
- Page 3, line -13: "a [n,k]". This should be "an [n,k]", since when pronouncing the letter n, one starts with a vowel sound.
- Page 6, line 4: In the second upper bound for the dimension of the Schur square of a trace code in Corollary 1.8, a pair of brackets is missing. More precisely, the formula $m \cdot dimC^2 - \binom{dim(C)+1}{2}$ should be $m \cdot \left(dimC^2 - \binom{dim(C)+1}{2}\right)$
- Page 6, proof of Corollary 1.10: In the proof an upper bound on the dimension of $Tr(C)^2$ is given in a series of formulas involving four $\leq$ signs. Actually the final three inequalities are equalities. It would be easier for the reader to replace these three inequalities with equalities.
- Page 7, line 1: "belong to" should be "belongs to"
- Page 7, Definition 13: the constants α_{0a} and α_{b0} are not allowed to be zero. Please add this condition.
- Page 7, Equation 10: The notation $\mathcal{O}_{P_\infty}$ for the ring $\cup_{s\geq 0} L(sP_\infty)$ is quite misleading. It is very common to use the notation $\mathcal{O}_{P_\infty}$ for the local ring at P_∞. This is the ring consisting of all functions that do not have a pole atP_∞. The authors consider in some sense the opposite situation: the ring of all functions with no poles except possibly at P_∞. Please use some other notation.
- Page 7, line -4: "$f = x^\beta y^\alpha + f'(x, y)$". The authors write that any $f \in \cup_{s\geq 0} L(sP_\infty)$ can be written in this form, but this is strictly speaking not true. One needs to allow for a leading coefficient different from one as well. Please write something like "$f = c \cdot x^\beta y^\alpha + f'(x, y)$ for some nonzero c." This also affects the leading term expression later on.
- Page 8, Remark 1.15: "It is worth noting that $\mathcal{O}_{P\infty}$ is a valuation ring with valuation v_{P_∞}". This is not true. Indeed, the only valuation ring with valuation v_{P_∞} is the local ring at P_∞. Please modify the remark. It is true that $\deg_{a,b}(f) = -v_{P_\infty}(f)$, which is perhaps the main point of the remark.
- Page 8, Definition 2.1: Later on the notation G is used for the divisor D+(g). It would help the reader if this is mentioned already here, since later on, for example in Remark 2.2, the notation G is used without explanation.
- Page 9, line 6: "for the good choice of divisor". I think the authors mean something like "for an appropriate choice of the divisor"
- Page 10, line 3: In the second summation in this line, there is "$\dim_{F_q}$" missing in front of the code $Tr(C * C^{q^i})$
- Page 11, line 2: The formula "$C_1 \subseteq C^{q^i} \cap C^{q^{m-1}}$" should be "$C_1 \subseteq C \cap C^{q^{m-1}}$".
- Page 11, line 4: "$Tr(C * C_1^{q^i}) \subseteq ...$"$shouldbe$"$Tr(C_1 * C_1^{q^i}) \subseteq ...$"
- Page 11, line 7: in the formula involving the intersection of summations of certain trace codes, the right-hand side is the empty set symbol. Since any code contains 0, I suspect the right-hand side should have been $\{0\}$ instead of $\emptyset$.
- Page 11, Remark 2.8: what is the parameter r? It is probably the degree of g, but I do not recall the authors mentioned this earlier. Please add a short explanation.
- Page 11, Proposition 3.2: Since g is the element one wants to divide by (with remainder), I needs to add the condition that $g \neq 0$.
- Page 12, Lemma 3.3: Previously the trace function Tr was only used and defined for elements from a finite field with q^m elements, but now it is applied to a function. This means that not longer $Tr(f) = Tr(f^q)$. However, this is used in the proof of the lemma. There is little harm, since later on the results are not applied to

functions but to codewords corresponding to them. Please explain briefly before the lemma what exactly is meant with $Tr(f)$ is f is a function, or reformulate in terms of codewords.

- Page 13, first line after Definition 3.2. "Lemma 3.3 entails that ...". Lemma 3.3 only applies to $i \geq 1$. Please add a short remark concerning the case i=0.
- Page 13, second line after Definition 3.2: "$Tr(f/q^{i+1})$" should be "$Tr(f/g^{q^i+1})$"
- Page 13, last line before subsection 3.3: "the trace codes $T_i(s, g)$". The sets $T_i(s, g)$ were defined in Definition 3.2 as sets of functions and not as codes. Did I misunderstand something? Please clarify.