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 into 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 3.9 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. TO DO: Answer this and be polite.
- Please give more clear comparisons and show the clear advantages of this paper. Add 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.

  We added two more tables to compare our construction with binary Goppa codes and 1–point Hermitian codes. We also added 2 examples in Section 2.

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

Typos and spelling mistakes have been corrected. Major modifications are listed bellow.

- Page 1. Subfield subcodes of AG codes. Line -7. Note the symbols of codes and curve. Check the use of $\mathcal{C}$ and C;

  We corrected the use of caligraphical letter in $C_{a,b}$, and we also add some context about the definition of the AG code $\mathcal{C}$. The notation $\mathcal{C}$ always represents a code, while $\mathcal{X}$ is reserved for curves.
- Page 2. It is better to give a clear description of the advantages of the upper bound of the dimension of codes.

  TO DO: Dire pourquoi une borne sur la dimension fournit un distingueur. Rajouter quelques lignes dans l'intro.
- Page 5. Please check the use of $\mathrm{Tr}(\mathcal{C})^{\star 2}$ and $\mathcal{C}^{q^i}$. It seems that $\mathrm{Tr}(\mathcal{C})^{\star 2}$ means $\mathrm{Tr}(\mathcal{C}^{\star 2})$. Many similar problems in the paper.

  At this point, we really want to talk about the square of the trace and not the trace of the square. To make it more readable, we changed the notation of the Trace by removing the underscore $\mathbb{F}_{q^m}/\mathbb{F}_q$ once correctly defined (i.e. after Equation (1)).

  Please give a description of $\mathcal{C}^{q^i}$.

  We added a description below Equation (6).
- Page 6. Note that $\deg G = s$. There are many symbols in the paper. Please give a clear description.

  The definition of the degree of a divisor can be found at page 4. We also changed the notation $\deg G$ into $\deg(G)$ where it was not already the case.

- Page 11. It is better to give some examples at the end of Section 2;
  We added Example 1 to compare bith Cartier and Goppa-like construction. We present 2 cases: an equality one and an inequality one. TO DO: Add another example after Proposition 2.6 to illustrate it.
- Page 18. Check the format of references. Update Reference [MT21].
  TO DO: script Python.

Second review's comment

Typos and spelling mistakes have been corrected. Major modifications are listed bellow.

- 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 $m \cdot dim_{\mathbb{F}_{q^m}} \mathcal{C}^{\star 2} - \binom{dim_{\mathbb{F}_{q^m}} \mathcal{C}+1}{2}$ should be $m \cdot \left(dim_{\mathbb{F}_{q^m}} \mathcal{C}^{\star 2} - \binom{dim_{\mathbb{F}_{q^m}} \mathcal{C}+1}{2} \right)$
  We add the missing bracket.
- Page 6, proof of Corollary 1.10: In the proof an upper bound on the dimension of $\mathrm{Tr}(\mathcal{C})^{\star 2}$ 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.
  We took you remark into account and changed the proof accordingly.
- Page 7, Definition 13: the constants α_{0a} and α_{b0} are not allowed to be zero. Please add this condition.
  The conditions have been added.
- Page 7, Equation 10: The notation $\mathcal{O}_{P_\infty}$ for the ring $\cup_{s\geq 0}\mathcal{L}(sP_\infty)$ 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.
  Thank you for pointing out this mistake. We changed the notation $\mathcal{O}_{P_\infty}$ into $\mathcal{S}$ which actually is the coordinate ring of the affine curve $\mathcal{X}_{a,b} \setminus \{P_\infty\}$. We changed the rest of the paper accordingly to this new notation.
- Page 7, line -4: "$f = x^\beta y^\alpha + f'(x,y)$". The authors write that any $f \in \cup_{s\geq 0}\mathcal{L}(sP_\infty)$ 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.
  We add a nonzero constant c in front of the expression and we also changed the expression of the leading monomial $\mathrm{LM}(f)$ *(note that we changed* $\mathrm{LT}(f)$ *into* $\mathrm{LM}(f)$*).*
  + TO DO: ajout remarque du fait qu'on travaille sur un corps, donc ça reviens essenciellement au même
- Page 8, Remark 1.15: "It is worth noting that $\mathcal{O}_{P_\infty}$ is a valuation ring with valuation ν_{P_∞}". This is not true. Indeed, the only valuation ring with valuation ν_{P_∞} is the local ring at P_∞. Please modify the remark. It is true that $\deg_{a,b}(f) = -\nu_{P_\infty}(f)$, which is perhaps the main point of the remark.
  We changed the remark, only keeping the link between the valuation at P_∞ and the weighted degree.
- 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.

The definition of G has been added before Definition 2.1.

- Page 10, line 3: In the second summation in this line, there is "$\dim_{F_q}$" missing in front of the code $\mathrm{Tr}\Big(\mathcal{C} \star \mathcal{C}^{q^i}\Big)$.

  The missing dimension has been added.
- Page 11, line 2: The formula "$\mathcal{C}_1 \subseteq \mathcal{C}^{q^i} \cap \mathcal{C}^{q^{m-1}}$" should be "$\mathcal{C}_1 \subseteq \mathcal{C} \cap \mathcal{C}^{q^{m-1}}$".

  The formula has been corrected.
- Page 11, line 4: "$\mathrm{Tr}\Big(\mathcal{C} \star \mathcal{C}_1^{q^i}\Big) \subseteq ...$" should be "$\mathrm{Tr}\Big(\mathcal{C}_1 \star \mathcal{C}_1^{q^i}\Big) \subseteq ...$"

  Actually, the result works with both $\mathcal{C}_1$ and $\mathcal{C}$. In the proof, we added a explanation "By taking th star product ..." to make it clearer.
- 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 $\varnothing$.

  The symbol has been changed.
- 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.

  We added a reference to classical Goppa codes (Equation (14)). Here, r is the order of the Goppa code.
- Page 11, Proposition 3.3: Since g is the element one wants to divide by (with remainder), I needs to add the condition that $g \neq 0$.

  The condition on g has been added. We also add Definition 3.2 : it allows us to introduce the notation $\mathcal{R}(h)$ for any function $h \in \mathcal{S}$ as we use it for several functions later on.
- Page 12, Lemma 3.4: 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 $\mathrm{Tr}(f) = \mathrm{Tr}(f^q)$. 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.

  We added a discussion before Lemma 3.4 (see. Section 3.3) to explain what we mean by the trace of a function: first, we extend the evaluation map $\mathrm{ev}_{\mathcal{P}}$ to the ring $\mathcal{S}$ as well as the trace operator by setting $\mathrm{Tr}(f) := f + f^q + \cdots + f^{q^{m-1}}$. Then, given $f, f' \in \mathcal{S}$, we say that $f \equiv_{\mathcal{P}} f'$ if $\mathrm{ev}_{\mathcal{P}}(f) = \mathrm{ev}_{\mathcal{P}}(f')$. Hence, we have $\mathrm{Tr}(f^q) \equiv_{\mathcal{P}} \mathrm{Tr}(f)$ (see Equation (16)). In particular, we have equality of the corresponding evaluation codewords. These new notation are then used for the rest of the paper.
- Page 13, first line after Definition 3.5. "Lemma 3.4 entails that ...". Lemma 3.4 only applies to $i \geq 1$. Please add a short remark concerning the case $i = 0$.

  A short remark for the case $i = 0$ has been added.
- Page 13, second line after Definition 3.5: "$\mathrm{Tr}\Big(\frac{f}{q^{i+1}}\Big)$" should be "$\mathrm{Tr}\Big(\frac{f}{g^{q^i+1}}\Big)$".

  The mistake has been corrected.
- Page 13, last line before Subsection 3.4: "the trace codes $\mathcal{T}_i(s, g)$". The sets $\mathcal{T}_i(s, g)$ were defined in Definition 3.5 as sets of functions and not as codes. Did I misunderstand something? Please clarify.

  We changed the definition of the $\mathcal{T}_i(s, g)'s$ (see Definition 3.5). They are now defined as codes whose codewords are the evaluation at the set of points $\mathcal{P}$ of traces of functions. Hence, the terminology "trace codes" makes sense.