

# 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:

**TO DO:** On a tenu compte de toutes les typos et fautes d'orthographes. Chacun des points plus compliqués sont détaillés. De plus, on a tenu compte des remarques des rapporteurs

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

**DONE:** We corrected the use of caligraphical letter in  $C_{a,b}$ , and we also add some context about the definition of the AG code  $\mathcal{C}$ .

- **TO DO:** Dire pourquoi une borne sur la dimension fournit un distinguoir: Page 2. It is better to give a clear description of the advantages of the upper bound of the dimension of codes.

- 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.

**DONE:** Actually it is really 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  $\mathbb{F}_{q^m}/\mathbb{F}_q$ .

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

**DONE:** We added a description below equation (5).

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

**DONE:** 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.

- **TO DO:** Mettre un exemple avant la sous-section 2.2 avec un cas égalité ou inégalité entre Goppa-like et Cartier. Reprendre le même exemple après 2.6 dans le cas ou la borne n'est effectivement pas atteinte, i.e. quand  $g$  est une puissance  $q$ -ème i.e.  $\mathcal{C}_1$  : Page 11. It is better to give some examples at the end of Section 2;
- **TO DO:** script Python : Page 18. Check the format of references. Update Reference [MT21].

## SECOND REVIEW'S COMMENT

TO DO: on a tenu compte de toutes les typos et fautes d'orthographes. Chacun des points plus compliqués sont détaillés.

- DONE: 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  $m \cdot \dim C^2 - \binom{\dim(C)+1}{2}$  should be  $m \cdot \left( \dim C^2 - \binom{\dim(C)+1}{2} \right)$
- DONE: Page 6, proof of Corollary 1.10: In the proof an upper bound on the dimension of  $\text{Tr}(C)^2$  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.
- DONE: the condition have been added : Page 7, Definition 13: the constants  $\alpha_{0a}$  and  $\alpha_{b0}$  are not allowed to be zero. Please add this condition.
- DONE: changer la notation de  $\mathcal{O}_\infty$  parce que c'est pas le bon truc. Est-ce que ça a un autre nom ? : 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  $P_\infty$ . This is the ring consisting of all functions that do not have a pole at  $P_\infty$ . The authors consider in some sense the opposite situation: the ring of all functions with no poles except possibly at  $P_\infty$ . 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. DONE: We took the modification into consideration. We also changed the notation of  $\text{LT}(f)$  into  $\text{LM}(f)$  + TO DO: ajout remarque du fait qu'on travaille sur un corps, donc ça revient essentiellement au même
- DONE: À modifier un peu après avoir modifier la notation  $\mathcal{O}_{P_{\text{inf}}}$  : enlever tout ce qui mentionne l'anneau de valuation à l'infini : Page 8, Remark 1.15: "It is worth noting that  $\mathcal{O}_{P_\infty}$  is a valuation ring with valuation  $v_{P_\infty}$ ". This is not true. Indeed, the only valuation ring with valuation  $v_{P_\infty}$  is the local ring at  $P_\infty$ . 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.
- DONE: The definition of  $G$  has been added right before Definition 2.1 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.
- DONE: The missing dimension has been added : Page 10, line 3: In the second summation in this line, there is " $\dim_{F_q}$ " missing in front of the code  $\text{Tr}(C * C^{q^i})$
- DONE: The formula has been corrected: Page 11, line 2: The formula " $C_1 \subseteq C^{q^i} \cap C^{q^{m-1}}$ " should be " $C_1 \subseteq C \cap C^{q^{m-1}}$ ".
- TO DO: Le résultat est vrai en l'état avec  $\mathcal{C}$ . C'est aussi vrai avec  $\mathcal{C}_1$  mais on s'en moque. L'expliquer : on a ajouter un peu de détails Page 11, line 4: " $\text{Tr}(C * C_1^{q^i}) \subseteq \dots$ " should be " $\text{Tr}(C_1 * C_1^{q^i}) \subseteq \dots$ "
- DONE: The symbol has been changed : 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  $\emptyset$ .
- DONE: We added a reference to classical Goppa codes as defined at the bottom of page 8 (i.e. Equation (13)). Here,  $r$  is the order of the Goppa code : 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.

- DONE: The condition on  $g$  has been added : Page 11, Proposition 3.2: Since  $g$  is the element one wants to divide by (with remainder), I needs to add the condition that  $g \neq 0$ .
- TO DO: Page 12, Lemma 3.3: Previously the trace function  $\text{Tr}$  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  $\text{Tr}(f) = \text{Tr}(f^q)$ . 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  $\text{Tr}(f)$  is  $f$  is a function, or reformulate in terms of codewords.
- TO DO: we added a 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  $i=0$ .
- DONE: Corrected : Page 13, second line after Definition 3.2: " $\text{Tr}(f/q^{i+1})$ " should be " $\text{Tr}(f/g^{q^{i+1}})$ "
- TO DO: Défined as codes : 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.