Ответ на рецензию статьи

"О ядрах нелинейных квазисовершенных кодов"

В первую очередь хочу выразить благодарность Рецензенту за внимательное прочтение работы и сделанные замечания и ценные предложения.

1) Стр. 146, строка 14. Грамматика: "может опускается".

Исправлено.

2) Стр. 146. Предложение "Нет известных кодов, связанных с кодом Вагнера, и код Вагнера, по-видимому, не является примером какого-либо более широкого класса кодов"не совсем точно. В работе Семакова Н.В., Зайцева Г.В. и Зиновьева В.А. (Zaitsev G.V., Zinoviev V.A., Semakov N.V., Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes, "Proc. of Second International Symposium on Information Theory (Tsahkadsor, Armenia, USSR, September,1971), Budapest, Academiai-Kiado, 1973, pp. 257-263.) построен бесконечный класс квазисовершенных кодов с расстоянием 5, который включает код Вагнера.

Исправлено.

3) Стр. 146, последний абзац. Имеются пересечения с работой [12] и с работой (Carlet, C., Charpin, P., and Zinoviev, V., Codes, Bent Functions and Permutations Suitable for Deslike Cryptosystems, Des. Codes Cryptogr., 1998, vol. 15, no. 2, pp. 125–156), которые надо точно указать.

Стр. 146. Предпоследний абзац

"Пусть $q = p^m$, причём $m \geq 3$. Пусть π — примитивный элемент поля $\mathbb{F}_q$ и $j = 0, 1, \ldots, q-2$. Пусть f — отображение из $\mathbb{F}_q$ в себя и $\mathcal{C}_f$ — линейный код длины $q-1$, проверочная матрица которого имеет столбец $\begin{bmatrix} \pi^j \\ f(\pi^j) \end{bmatrix}$ в качестве своего j-го столбца. Ли и Хеллесет [9] показали, что в случае $p = 2$ код $\mathcal{C}_f$ имеет радиус покрытия 3, когда f является квадратичной APN-функцией. Это дает возможность построить ряд квазисовершенных двоичных кодов с минимальным расстоянием 5. В случае, когда p — нечётное простое число, в [9] доказано, что для всех известных планарных функций f радиус покрытия кода $\mathcal{C}_f$ равен 2, если m нечётное, и 3, если m чётное. В результате было получено несколько классов квазисовершенных p-ичных кодов."

Это просто аннотация статьи [9]. И что там с чем пересекается это забота авторов статьи [9] или отдельного исследования.

Стр. 146. Последний абзац

"Ли и Хеллесет [9] представили ряд открытых вопросов, связанных с квазисовершенными кодами и криптографическими функциями."

Что имеется ввиду?

4) Стр. 148, второй абзац. В рамках той же темы напрашивается ссылка на работу (Borges J., Phelps K.P., Rifa J., and Zinoviev V.A., On Z_4-linear Preparata-like and Kerdock-like codes, "IEEE Trans. On Information Theory 2003, v. 49, No. 11, pp. 2834 - 2843), которая неи содерэит вычислений на компьютере.

Стр. 148, второй абзац. "Вопрос о ранге и размерности ядра является естественным для нелинейных кодов и связан с классификацией кодов. Ранг и размерность ядра изучались, например, для совершенных кодов, кодов Адамара, Z_2Z_4-линейных кодов, $Z_pZ_{p^2}$-линейных кодов [16, 17, 18, 19, 19a, 20]. В [21] изучались ранг и размерность ядра некоторых подклассов квазисовершенных двоичных кодов."

Перечислены примеры работ, в которых рассматриваются вопросы о ранге и размерности ядра. Таких примеров существует много и приведенных в моей работе вполне достаточно.

5) Стр. 150, последнее предложение перед разделом 3. Указать параметры кодов. Сравнить с кодами из семейства (F.41) из [12] (см. стр. 42)

Параметры кодов указаны.

Что касается кодов из семейства (F.41), то авторы семейства (F.41), по-видимому, построили коды эквивалентные обобщенным кодам Рида-Маллера порядка $r = (q-1)m-2$ в терминах дуальных кодов. Но авторы семейства (F.41), по-видимому, не знали, что открытые ими коды это обобщенные коды Рида-Маллера порядка $r = (q-1)m-2$. Вопрос эквивалентности конечно остается открытым и требует изучения. Моя статья посвящена квазисовершенным кодам, а не полностью регулярным. Не стоит грузить читателя.

6) Стр. 150, Первые 4 строки раздела 3. Матрица H введена неуклюже. Почему не так: "Столбцами матрицы H являются все возможные векторы длины m+1 над полем F_q первая позиция которых равна 1. что короче и понятней.

Дано новое определение.

7) Стр. 151, Предложение 1. Написать длину n в явном виде. Хорошо бы иметь здесь параметры кода R_i.

Исправлено.

8) Стр. 152, седьмая строка перед Теоремой 1. Опечатка: Нужно "$[m]_q$". Такое же замечание относится к последней строке на стр. 152.

Исправлено.

9) Стр. 152, Теорема 1, Сравнить коды с кодами из из семейства (F.41) из [12] (см. стр. 42) Вопрос об эквивалентности кодв из [9] и кодов остается открытым.

Семейства (F.41) это линейные коды.

Работа [9] C. Li, T. Helleseth, *Quasi-perfect linear codes from planar and APN functions*, Cryptogr. Commun., **8**:2 (2016), 215–227.

Я рассматриваю нелинейные коды.

10) Стр. 153, строка 2: "мымы".

Исправлено.

11) Стр. 153, конструкция, описываемая Теоремой 2. Имеется пересечение с работой (J. Borges, J. Rifa, V.A. Zinoviev, On completely regular and completely transitive supplementary codes, Discrete Math. 343(3) (2020) 111732), где для конструкции используется та же идея.

Теорема 2 и теоремой 3 получаются путём применения теоремы 1 к результатам работы K.T. Phelps, J. Rifa, M. Villanueva, *Kernels and p-kernels of p^r-ary 1-perfect codes*, Des. Codes Cryptogr., **37**:2 (2005), 243–261.

Возможно имеется ввиду теорема 1 ?

Какое-то пересечение идей возможно и можно увидеть.

Исправлено. Добавлена ссылка на работу (J. Borges, J. Rifa, V.A. Zinoviev, On completely regular and completely transitive supplementary codes, Discrete Math. 343(3) (2020) 111732)