# Краткое изложение заявки

# Алгебраическая иерархия транзитивных кодов

**Заявитель: Могильных Иван Юрьевич**

Данный проект направлен на исследование иерархии кодов исправляющих ошибки в канале связи с шумами, а именно транзитивных кодов с параметрами кодов Хэмминга, Препараты и Кердока.

С кодом в метрическом пространстве Хэмминга, где свяжем *группу автоморфизмов* – стабилизатор кода как множества в группе изометрий пространства. Отдельно можно выделить *транзитивные* коды – группа автоморфизмов которых содержит подгруппу действующую транзитивно на кодовых словах. Если подгруппа $H$ является *регулярной* (то есть ее порядок совпадает с мощностью кода), то такой код назовем кодом с *регулярным представлением* группой $H$ (в англоязычной литературе такой код называется propelinear). Отметим что для заданного кода может существовать большое количество его регулярных представлений, в том числе неизоморфных. Исключительностью понятия кода с регулярным представлением $H$ является то, что оно позволяет определить на множестве элементов такого кода естественным образом групповую операцию изоморфную $H$, отличную от наследуемой основной операции пространства Хэмминга. Таким образом коды с регулярными представлениями обобщают все ранее известных групповые способы задания кодов, исправляющих ошибки, такие как коды линейные, Z4-линейные (первый $Z4$-линейный код Кердока построен А.А.Нечаевым) и Z2Z4-линейных кодов.

В свою очередь, регулярное представление некоторого кода группой $H$ с нормальной подгруппой, назначенной кодовым словам из максимального линейного подпространства кода $C$ в пространстве Хэмминга назовем *нормализованным*, а сам код имеющим *нормализованное регулярное представление*.

**Главной задачей** данного проекта является выяснение иерархии вложимости определенных выше понятий (транзитивных, кодов с регулярным и нормализованным регулярным представлениями) в классах кодов с хорошими характеристиками (например, оптимальных кодов, таких как совершенные, Препараты и Кердока).

В 2012 году заявителем проекта было показано, что оптимальный код Беста длины 10 является транзитивным, не имеющим регулярного представления, для класса совершенных кодов такой пример также был получен совсем недавно в сентябре 2013 года для первой нетривиальной длины $n = 15$. В рамках проекта планируется получение обобщения данного результата в классе совершенных кодов для любой фиксированной допустимой длины $n$ и других классов оптимальных кодов.

С другой стороны, все известные на сегодняшний день конструкции кодов с регулярным представлением допускают нормализованное регулярное представление. Более того, известно, что существуют коды, которые допускают лишь нормализованное регулярное представление. В данном проекте предлагается показать существование бесконечной серии кодов с регулярным ненормализованным представлением.

В ходе исследования предлагается прояснить скрытую алгебро-комбинаторную сторону отношений вложимости введенных понятий, построение новых транзитивных кодов и кодов с регулярными и нормализованным регулярным представлениями, их инвариантов и свойств.

Данные исследования представляют интерес с теоретической точки зрения алгебро-комбинаторной теории кодирования, а также интересны с точки зрения криптографии, поскольку большое количество регулярных неизоморфных представлений даже одного кода могут найти применение в асимметричной криптографии, а именно в аналогах криптосистем МакЭлиса и Нидеррайтера, использующих коды исправляющие ошибки.