О НОРМЕННОМ МЕТОДЕ РЕШЕНИЯ УРАВНЕНИЙ В ПОЛЯХ ГАЛУА

В.А. Липницкий, Н.В. Спичекова

Решение алгебраических уравнений над полями Галуа является одним из необходимых этапов во многих процедурах помехоустойчивого декодирования, криптографии, задачах теоретической физики и так далее.

На рубеже XX и XXI веков белорусской школой кодирования разработана теория норм синдромов, следствием которой являются эффективные методы коррекции ошибок циклическими кодами. Другим следствием теории являются норменный метод решения

уравнений в полях Галуа. Данный метод предполагает объединение уравнений в условные Г-орбиты по следующему отношению: если множество корней одного уравнения можно получить из такого же множества корней другого уравнения умножением на примитивный элемент поля Галуа, то уравнения они эквивалентны и принадлежат одной Г-орбите. Норменный метод предназначен для ситуаций с многократным решением уравнений данной степени. Для его реализации составляется список всех орбит уравнений данной степени с наипростейшими характеристиками каждой орбиты. Решение уравнения осуществляется вычислением нормы этого уравнения, нахождением нормы в составленном списке и стандартной методикой определения корней данного уравнения внутри орбиты.

В докладе рассматривается модернизация норменного метода, позволяющая существенно сократить необходимый список Г-орбит для реализации норменного метода.