Journal of Pure and Applied Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Maximal order codes over number fields

Christian Maire [a], Frédérique Oggier [b,*]

[a] *Laboratoire de Mathématiques de Besançon, Université Bourgogne Franche-Comté et CNRS (UMR 6623), 16 route de Gray, 25030 Besançon cédex, France*
[b] *Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore*

ARTICLE INFO

Article history:
Received 2 February 2017
Received in revised form 18 July 2017
Available online xxxx
Communicated by I.M. Duursma

MSC:
11T71; 94B40; 11R52; 94B75

ABSTRACT

We present constructions of codes obtained from maximal orders over number fields. Particular cases include codes from algebraic number fields by Lenstra and Guruswami, codes from units of the ring of integers of number fields, and codes from both additive and multiplicative structures of maximal orders in central simple division algebras. The parameters of interest are the code rate and the minimum Hamming distance. An asymptotic study reveals several families of asymptotically good codes.

1. Preliminaries

Given

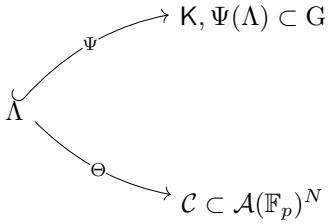
(i) a number field $\mathbb{K}$ and a maximal order (or a subgroup of the units of a maximal order) Λ defined on $\mathbb{K}$;
(ii) a locally compact group G and K a compact of G;
(iii) an embedding $\Psi : \Lambda \hookrightarrow \mathsf{G}$ such that the image $\Psi(\Lambda)$ is a lattice of G, *i.e.* a discrete subgroup with a fundamental domain of finite measure;
(iv) a map $\Theta : \Lambda \to \mathcal{A}(\mathbb{F}_p)^N$ where $\mathcal{A}(\mathbb{F}_p)$ is an alphabet over the finite field $\mathbb{F}_p$, p a prime, and $N \geq 1$ is an integer,

we consider the code $\mathcal{C} = \Theta\big(\Psi^{-1}(z\mathsf{K} \cap \Psi(\Lambda))\big)$, for some z in a given fundamental domain of $\Psi(\Lambda)$.

* Corresponding author.
E-mail addresses: christian.maire@univ-fcomte.fr (C. Maire), frederique@ntu.edu.sg (F. Oggier).

http://dx.doi.org/10.1016/j.jpaa.2017.08.009
0022-4049/

Please cite this article in press as: C. Maire, F. Oggier, Maximal order codes over number fields, J. Pure Appl. Algebra (2017), http://dx.doi.org/10.1016/j.jpaa.2017.08.009



Codewords of the code $\mathcal{C}$ are elements of $\mathcal{A}(\mathbb{F}_p)^N$, and the parameters of interest are

- the rate $\frac{\log_q |\mathcal{C}|}{N}$ of the code, where $q = |\mathcal{A}(\mathbb{F}_p)|$, N is the code length, and $\log_q(x) = \ln x/\ln q$;
- its minimum Hamming distance $d_H(\mathcal{C})$ which counts the minimum number of components in which any two distinct codewords differ.

The goal is to obtain both a high rate and a high minimum distance. The trade-off between both is characterized by the Singleton bound, which for nonlinear codes states that

$$\log_q |\mathcal{C}| \leq N - d_H(\mathcal{C}) + 1.$$

Asymptotically, the relative minimum distance $d_H(\mathcal{C})/N$ is considered, and families of codes $(\mathcal{C}_i)_i$ with length N_i that satisfy

$$\liminf_i \frac{\log_q |\mathcal{C}_i|}{N_i} > 0, \quad \liminf_i \frac{d_H(\mathcal{C}_i)}{N_i} > 0,$$

are called *asymptotically good codes*, e.g. [30, Chapter I, §1.3]. The alphabet size could more generally be allowed to grow with i, though we consider codes for which q is constant, which are of special interest.

A first instance of the above principle is the code construction from algebraic number fields due to Lenstra [12] (and rediscovered independently by Guruswami [3]). An asymptotic analysis of this code instance was provided in both works, and asymptotically good codes were found.

Example 1. [Lenstra [12], Guruswami [3]] Let $\mathbb{K}$ be a number field of degree n with infinite places $\mathbb{P}_\infty$ and let $\mathcal{O}_\mathbb{K}$ be its ring of integers. Set $\Lambda = \mathcal{O}_\mathbb{K}$. Take Ψ to be the embedding of $\mathbb{K}$ in its archimedean completions, so that $\mathrm{G} = \prod_{\sigma\in\mathbb{P}_\infty} \mathbb{K}_\sigma \simeq \mathbb{R}^n$, and Θ the reduction modulo N distinct prime ideals of $\mathcal{O}_\mathbb{K}$ above p. Then $N \leq n$ and $\mathcal{A}(\mathbb{F}_p)$ is a finite extension of $\mathbb{F}_p$. In particular, $\mathcal{A}(\mathbb{F}_p) = \mathbb{F}_p$ when $N = n$.

Remark 1. It is also possible to consider prime ideals above different primes p, as done in [12,3], in which case Θ should be defined using $\prod_p \mathcal{A}(\mathbb{F}_p)$ rather than $\mathcal{A}(\mathbb{F}_p)^N$. This paper focuses on the case where all prime ideals are above the same prime, which is usually more standard [20, 1,§1–§2(vi)] from a coding theory view point, even though the results that will be proven hold in the general case.

A natural extension of Lenstra's construction is the Arakelov construction of Goppa codes from function fields by Nakashima [17,18]. Another extension of Goppa codes to division algebras in the function field situation can be found in a work by Morandi and Sethuraman [16]. Neither Nakashima nor Morandi and Sethuraman consider the asymptotic behavior of the codes.

This paper presents a generalization of the work by Lenstra and Guruswami, in the number field case. In particular, our framework gives rise to the following cases, whose details will be given later on in the paper.

Example 2. Firstly, we use the multiplicative structure of the ring of integers $\mathcal{O}_\mathbb{K}$, where $\mathbb{K}$ is a number field of signature (r_1, r_2). Take Λ to be the units of $\mathcal{O}_K$, $\Lambda = \mathcal{O}_\mathbb{K}^\times$. Then Ψ is the logarithmic embedding

Please cite this article in press as: C. Maire, F. Oggier, Maximal order codes over number fields, J. Pure Appl. Algebra (2017), http://dx.doi.org/10.1016/j.jpaa.2017.08.009