NUMBER THEORY AND ITS APPLICATIONS

Place and time: In M105 on Thursday, Jan 4, at 16:00–17:30
Organizer: Vesa Kaarnioja (University of Helsinki)
Contact email: vesa.kaarnioja@helsinki.fi

Well-rounded number theoretic lattices for wiretap channels

Oliver Gnilke *(Aalto University)*, oliver.gnilke@aalto.fi

Abstract. Wireless communications relies on the construction of lattices as codebooks. Depending on the channel model assumed different properties of these lattices relate to their usefulness in communications.

In this presentation we focus our attention on the single-input single-output (SISO) Rayleigh fading channel in a wiretap setting. We introduce lattices from number theoretic constructions as well as suitable sublattices for coset coding to protect against eavesdroppers.

It turns out that the information gain at the eavesdropper is described by the theta series of the lattice. We propose the class of well-rounded lattices to minimize the leakage of information and present simulations to support these claims.

On the inertia of an LCM matrix

Mika Mattila *(Tampere University of Technology)*, mika.mattila@tut.fi

Abstract. Let $S = \{x_1, x_2, \ldots, x_n\}$ be a set of distinct positive integers with $x_i \leq x_j \Rightarrow i \leq j$. The GCD matrix (S) of the set S is the $n \times n$ matrix with $\gcd(x_i, xj)$ as its ij entry. Similarly, the LCM matrix $[S]$ of the set S has $\operatorname{lcm}(x_i, x_j)$ as its ij entry. Both of these matrices were originally defined by H. J. S. Smith in his seminal paper from the year 1876.

During the last 30 years both GCD and LCM matrices (as well as their various generalizations) have been investigated extensively in the literature. However, GCD matrices are in many ways easier to study than LCM matrices. For example, the GCD matrix (S) is positive definite for any set S whereas the LCM matrix $[S]$ is almost always indefinite and may be even singular. Very little is known about the inertia of the matrix $[S]$ in general. One can of course make some additional assumptions about the set S, but still the matrix $[S]$ remains quite hard to study. In 1992 Bourque and Ligh conjectured that if the set S is GCD closed (that is, $\gcd(x_i, x_j) \in S$ for all $x_i, x_j \in S$), then the matrix $[S]$ is nonsingular. A few years later it was shown that this conjecture holds only for GCD closed sets with at most 7 elements, but not in general for larger sets.

It turns out that if the set S is GCD closed, then the poset-theoretic semilattice structure of $(S, |)$ often alone determines the inertia of the LCM matrix $[S]$ completely. This is a bit surprising, since one could expect the exact values of the elements $x_i \in S$ to play a bigger role in this. In this presentation we are going to define a new lattice theoretic concept and use it to give an explanation to this mystery. We also show some examples how to determine the inertia of the matrix $[S]$ by looking only at the semilattice structure of $(S, |)$.

Joint work with P. Haukkanen and J. Mäntysalo.

On Hong and Loewy's numbers and the Ilmonen–Haukkanen–Merikoski numbers

Vesa Kaarnioja *(University of Helsinki)*, vesa.kaarnioja@helsinki.fi

Abstract. Let K_n be the set of all nonsingular $n \times n$ lower triangular Boolean matrices. Hong and Loewy (2004) introduced the numbers

$$c_n = \min\{\lambda \mid \lambda \text{ is an eigenvalue of } XX^{\mathrm{T}},\ X \in K_n\}, \quad n \in \mathbb{Z}_+.$$

A related family of numbers was considered by Ilmonen, Haukkanen, and Merikoski (2008):

$$C_n = \max\{\lambda \mid \lambda \text{ is an eigenvalue of } XX^{\mathrm{T}},\ X \in K_n\}, \quad n \in \mathbb{Z}_+.$$

Both numbers appear, e.g., in the estimation of the spectral radii of GCD and LCM matrices and their lattice-theoretic generalizations.

In this talk, we present a new lower bound for the numbers c_n.

Theorem. *Let φ be the Golden ratio. For odd n, we have*

$$c_n \geq \frac{1}{\sqrt{\frac{1}{25}\varphi^{-4n} + \frac{2}{25}\varphi^{-2n} - \frac{2}{5\sqrt{5}}n\varphi^{-2n} - \frac{23}{25} + n + \frac{2}{25}\varphi^{2n} + \frac{2}{5\sqrt{5}}n\varphi^{2n} + \frac{1}{25}\varphi^{4n}}}.$$

For even n, we have

$$c_n \geq \frac{1}{\sqrt{\frac{1}{25}\varphi^{-4n} + \frac{4}{25}\varphi^{-2n} - \frac{2}{5\sqrt{5}}n\varphi^{-2n} - \frac{2}{5} + n + \frac{4}{25}\varphi^{2n} + \frac{2}{5\sqrt{5}}n\varphi^{2n} + \frac{1}{25}\varphi^{4n}}}.$$

This bound improves the estimates derived by Mattila (2015) and Altınışık et al. (2016). The sharpness of this lower bound is assessed numerically, which leads us to conjecture that $c_n \sim 5\varphi^{-2n}$ as $n \to \infty$.

In addition, we derive a closed form expression for C_n.

Theorem.

$$C_n = \frac{1}{4}\csc^2\left(\frac{\pi}{4n+2}\right) = \frac{4n^2}{\pi^2} + \frac{4n}{\pi^2} + \left(\frac{1}{12} + \frac{1}{\pi^2}\right) + \mathcal{O}\left(\frac{1}{n^2}\right).$$

An application of the formula for C_n is discussed within the context of the finite difference method.