

Otto-von-Guericke-Universität Magdeburg
Fakultät für Mathematik

Auf Einladung des Institutes für Algebra und Geometrie spricht

Herr Alexandr Polujan

(Otto-von-Guericke-Universität Magdeburg, IAG)

über das Thema

Homogeneous Cubic Bent Functions: From Known Examples to New Constructions

Ort: Otto-von-Guericke-Universität Magdeburg, Gebäude 02, Raum 20

Zeit: Dienstag, 2. Juli 2019, 13.00 Uhr

Zu diesem Vortrag laden wir alle Interessierten herzlich ein.

Abstract: Boolean bent functions, being opposite to affine functions, attracted a lot of attention from researchers of different areas in mathematics since their introduction in early 1960's. The problem of constructing homogeneous bent functions, which were originally introduced by [Qu, Seberry and Pieprzyk in 1999](#), arises from efficient evaluation of certain cryptographic algorithms. In 2002, [Charnes, Röttler and Beth](#) constructed around 700 examples of homogeneous cubic bent functions in 10 and 12 variables¹.

In this talk, after the survey of certain results about bent functions, we will deal with those, which are homogeneous and cubic. We will show, that some of the “lost” examples, being used as “building blocks” in a special secondary construction of bent functions, can produce homogeneous cubic bent functions, which:

- are different from the only one known analytic construction of [Seberry, Xia, Pieprzyk, 2000](#);
- do not belong to the completed Maiorana-McFarland class $\mathcal{M}^\#$. Thus we prove, that unlike the cases of 6 and 8 variables, the $\mathcal{M}^\#$ class does not describe the whole class of cubic bent functions in n variables for all $n \geq 16$. Further nontrivial analysis shows, that these functions also solve a recent problem on the existence of cubic bent functions without affine derivatives outside the $\mathcal{M}^\#$ class, proposed by [Mandal, Gangopadhyay and Stănică in 2017](#).

Finally, we will show, that in some cases one can construct a lot of “new building blocks”, provided that a “nice” single one is given.

This is [joint work](#) with [Alexander Pott](#).

¹We will call them “lost” since they are not available online anymore.