

On the Extended Feistel Networks and Their Quasigroups

Aleksandra Mileva
(joint work with Smile Markovski)

The extended Feistel networks (EFNs) are defined elsewhere. Here we give a further analysis of the EFNs and quasigroups produced by them. Among other things, we give the shape of the correlation matrices and prop ratio tables of the EFNs defined over the abelian group $(\mathbb{Z}_2^n, \oplus_n)$, as well as of the produced quasigroups. Some properties of the quasigroups produced by EFNs defined over other groups are investigated too.

Mathematics Subject Classification 2000: Primary 20N05; Secondary 94A60.

Keywords: Extended Feistel networks, huge quasigroups, correlation matrices, prop ratio tables.

Aleksandra Mileva:

Faculty of Informatics, "Goce Delčev" University, Štip, Republic of Macedonia
e-mail: aleksandra.mileva@ugd.edu.mk

Smile Markovski:

Institute of Informatics, Faculty of Natural Sciences and Mathematics,
"Ss Cyril and Methodius" University, Skopje, Republic of Macedonia
e-mail: smile@ii.edu.mk