Matrix representation of Bilinear Multivariate Quadratic Quasigroups of order 2^n

MARIJA MIHOVA*
*Ss. Cyril and Methodius University, Faculty of Computer Science and Engineering, Skopje

The quasigroup $(\{0,1\}^n, *)$ is called a Bilinear Multivariate Quadratic Quasigroups (BMQQ) if the quasigroup operation can be represented by a vector valued Boolean function $f(\overrightarrow{x}, \overrightarrow{y}) = \overrightarrow{z}$, where for some constants $c_k, a_{k_i}, b_{k_i} \in \{0,1\},\ k, i = \overline{1,n}$

$$z_k = c_k + \sum_{i=1}^{n} a_{k_i} x_i + \sum_{i=1}^{n} b_{k_i} y_i + \sum_{i=1}^{n} \sum_{j=1}^{n} d_{k_{ij}} x_i y_j \tag{1}$$

But, not every Boolean function yields a quasigroup. In this paper we determine the relation between the coefficients, so that the above inequality defines a quasigroup. Moreover, we analyze the relationship between the coefficients when the quasigroup is commutative and associative.