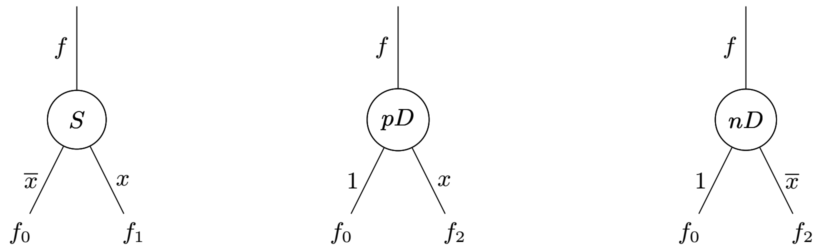
II INTERNATIONAL BALTIC SYMPOSIUM ON APPLIED AND INDUSTRIAL MATHEMATICS

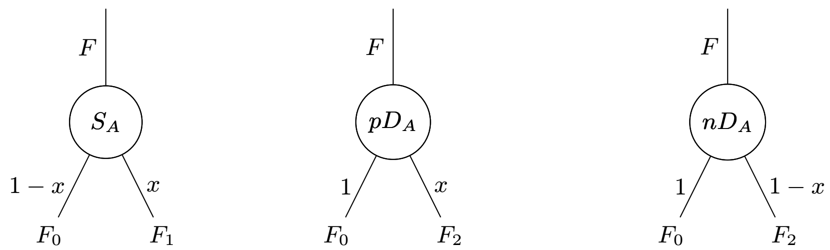
O. A. Finko, **K. S. Meretukov** (Krasnodar, KVVU). **Systems of Boolean functions: numerical decomposition in $\mathbb{Z}_m$ ring.**

Binary Decision Diagrams (BDD) [1] are built on the basis of Shennon decomposition, positive and negative Davio decompositions [2]. These diagrams are widely used for representation and realization of Boolean functions (BF) — «Bit level» — $f(x_1, x_2, ..., x_n)$:



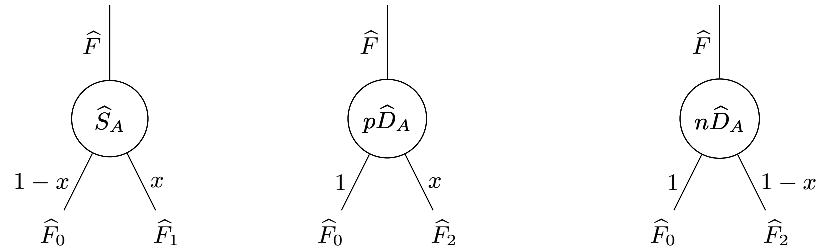
$$f = \overline{x} \wedge \underbrace{f_{|x=0}}_{f_0} \vee x \wedge \underbrace{f_{|x=1}}_{f_1} \quad f = \underbrace{f_{|x=0}}_{f_0} \oplus x \wedge \underbrace{(f_{|x=0} \oplus f_{|x=1})}_{f_2} \quad f = \underbrace{f_{|x=1}}_{f_1} \oplus \overline{x} \wedge \underbrace{(\overbrace{f_{|x=0}}^{f_0} \oplus \mathrm{f}_{|\mathrm{x}=1})}_{f_2}$$

In [2] arithmetic BDD are considered for realization of *BF systems* — «Word level» — $F(x_1, x_2, \ldots, x_n)$. The lower circle of BDD based on the arithmetic Shennon decomposition, represents numerical values of the right column of the table of BF system validity; the lower circle of BDD based on the arithmetic positive Davio decomposition consists of coefficients from $\mathbb{Z}$ polynoms received by generalization of a numerical normal form:



$$F = (1-x)\,\underbrace{F_{|x=0}}_{F_0} + x\,\underbrace{F_{|x=1}}_{F_1} \quad F = \underbrace{F_{|x=0}}_{F_0} + x\,\underbrace{(-F_{|x=0} + F_{|x=1})}_{F_2} \quad F = \underbrace{F_{|x=1}}_{F_1} + (1-x)\,\underbrace{(\overbrace{F_{|x=0}}^{F_0} - \mathrm{F}_{|\mathrm{x}=1})}_{F_2}$$

In [3] modular forms of arithmetic polynomials are invented. Following [3] arithmetic decomposition BF systems —«Word level» — in the ring $\mathbb{Z}_m$ ($\widehat{\oplus}$ — composition in $\mathbb{Z}_m$; $\widehat{F} \in \mathbb{Z}_m$) are considered:



$$\widehat{F} = (1-x)\underbrace{\widehat{F}_{|x=0}}_{\widehat{F}_0} \widehat{\oplus} x \underbrace{\widehat{F}_{|x=1}}_{\widehat{F}_1} \quad \widehat{F} = \underbrace{\widehat{F}_{|x=0}}_{\widehat{F}_0} \widehat{\oplus} x \underbrace{(-\widehat{F}_{|x=0} \widehat{\oplus} \widehat{F}_{|x=1})}_{\widehat{F}_2} \quad \widehat{F} = \underbrace{\widehat{F}_{|x=1}}_{\widehat{F}_1} \widehat{\oplus}(1-x)\underbrace{(\overbrace{\widehat{F}_{|x=0}}^{\widehat{F}_0} \widehat{\oplus}(-\widehat{\mathrm{F}}_{|x=1}))}_{\widehat{F}_2}$$

In some cases numerical decomposition of BF systems in the ring $\mathbb{Z}_m$, by analogy with modular polynomials from [3], makes it possible to reduce the temporary and/or spatial complexity of BF systems realization by supporting means for the asymmetric cryptoalgorithms (functioning in the ring $\mathbb{Z}_m$)and are applied to support implementers of symmetric cryptoalgorithms and other applications.

REFERENCES

1. *Bryant R. E.* Graph-based algorithms for Boolean functions manipulation. — IEEE Trans. Comput., 1986, v. C-35, is. 8, p. 677–691.
2. *Yanushkevich S. N.*, *Miller D. M.*, *Shmerko V. P.*, *Stankovic R. S.* Decision Diagram Technigues for Micro- and Nanoelectronic Design. Boca Raton, Fl.: CRC Press, 2006, 952 p.
3. *Fin'ko O.A.* Large systems of Boolean functions: realization by modular arithmetic methods. — Autom. Remote Control, 2004, v. 65, is. 6, p. 871–892.