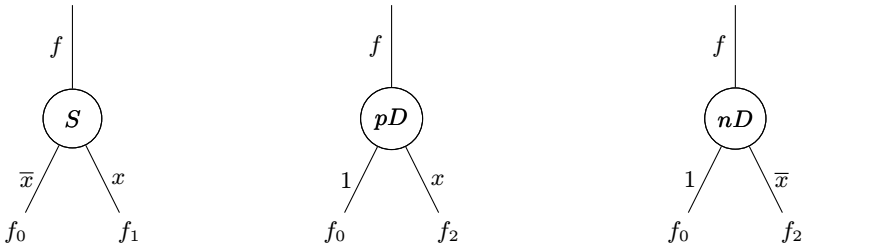
ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 5
2015

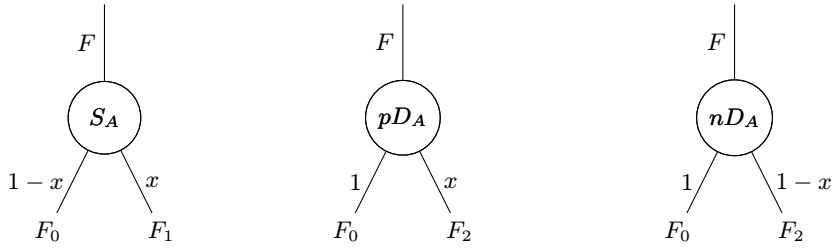
О. А. Финько, К. С. Меретуков (Краснодар, КВВУ). **Числовые разложения систем булевых функций в $\mathbb{Z}_m$.**

Binary Decision Diagrams (BDD) [1] строятся на основе разложений Шеннона, положительного и отрицательного разложений Давио [2] и нашли широкое применение для представления и реализации булевых функций (БФ) — «Bit level» — $f(x_1,\ldots,x_n)$:



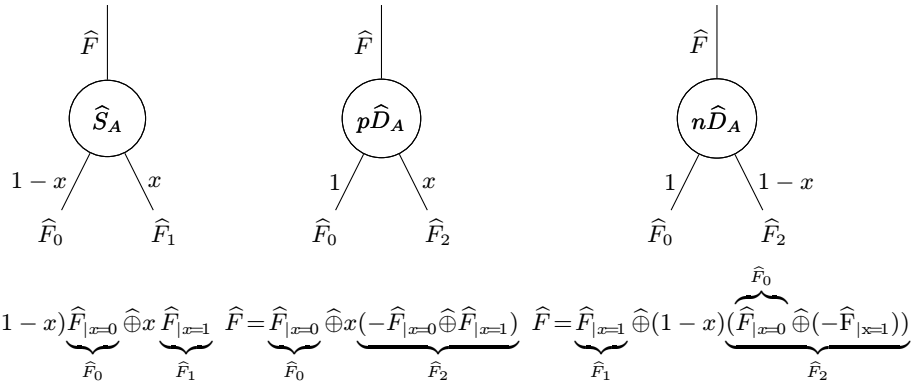
$$f=\overline{x}\wedge\underbrace{f_{|x=0}}_{f_0}\vee x\wedge\underbrace{f_{|x=1}}_{f_1}\quad f=\underbrace{f_{|x=0}}_{f_0}\oplus x\wedge\underbrace{(f_{|x=0}\oplus f_{|x=1})}_{f_2}\quad f=\underbrace{f_{|x=1}}_{f_1}\oplus\overline{x}\wedge\underbrace{(\overbrace{f_{|x=0}}^{f_0}\oplus f_{|x=1})}_{f_2}$$

В [2] рассмотрены арифметические BDD для реализации *систем* БФ — «Word level» — $F(x_1,\ldots,x_n)$. Нижний ярус BDD на основе арифметического разложения Шеннона, представляет собой числовые значения правого столбца таблицы истинности системы БФ; нижним ярусом BDD на основе арифметического положительного разложения Давио, являются коэффициенты из $\mathbb{Z}$ полинома, полученного обобщением числовой нормальной формы:



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

В [3] введены модулярные формы арифметических полиномов. Следуя [3] вводятся арифметические разложения систем БФ — «Word level» — в $\mathbb{Z}_m$ ($\widehat{\oplus}$ — сложение в $\mathbb{Z}_m$; $\widehat{F}\in\mathbb{Z}_m$):



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

Арифметические разложения систем БФ в $\mathbb{Z}_m$, по аналогии с модулярными полиномами из [3], позволяют в некоторых случаях уменьшать временную и/или пространственную сложность реализации систем БФ средствами поддержки асимметричных криптоалгоритмов (функционирующих в $\mathbb{Z}_m$) и применены для поддержки средств реализации симметричных криптоалгоритмов и других приложений.

СПИСОК ЛИТЕРАТУРЫ

1. *Bryant R. E.* Graph-based algorithms for boolean functions manipulation. — IEEE Transactios on Computers, 1986, v. 35, № 8.
2. *Yanushkevich S. N.*, *Miller D. M.*, *Shmerko V. P.*, *Stankovic R. S.* Decision diagram technigues for micro- and nanoelectronic design. Boca Raton, Florida: CRC Press, 2006, 952 p.
3. *Финько О. А.* Реализация систем булевых функций большой размерности методами модулярной арифметики. — Автомат. и телемех., 2004, № 6, с. 37–60.