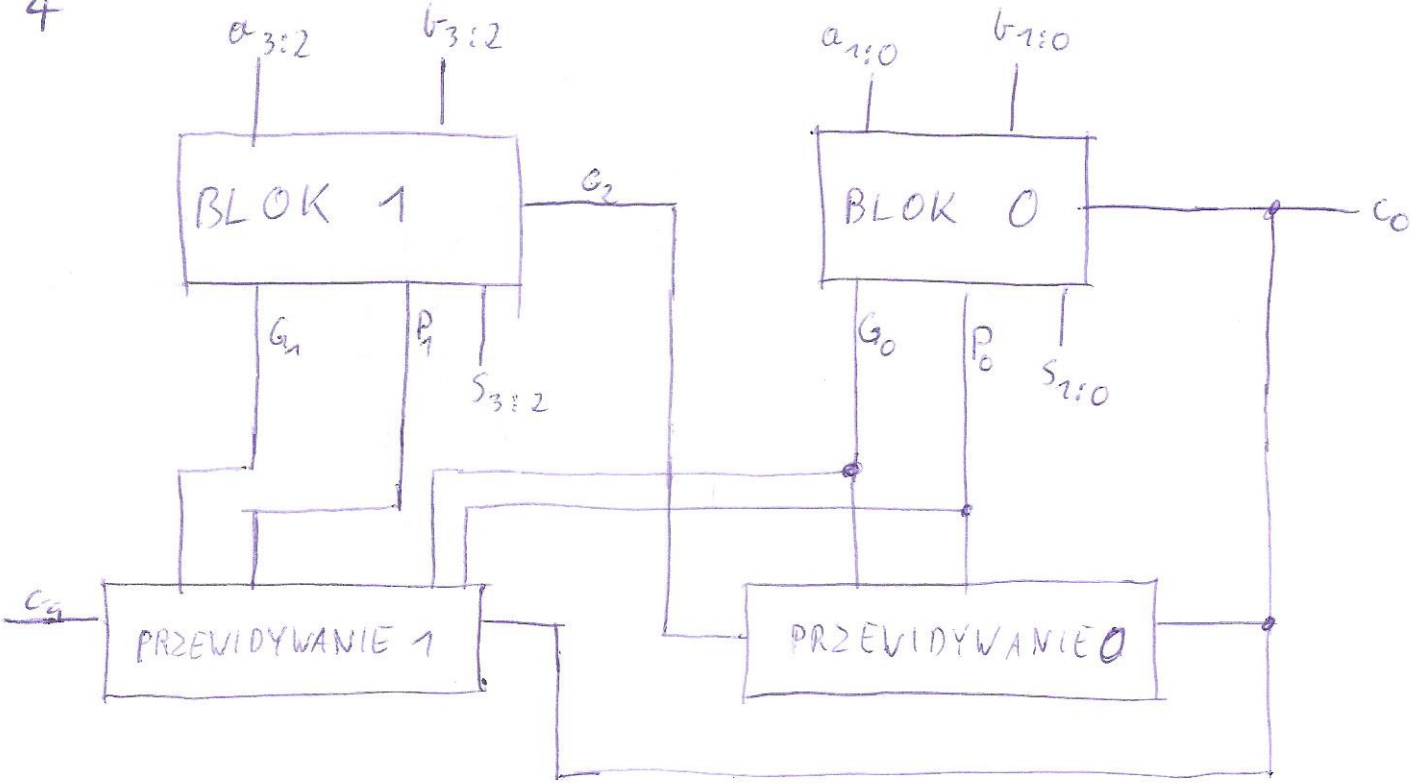
4



Z wzorów:

$s_k = a_k \oplus b_k \oplus c_k$

$c_n = g_{n-1} + p_{n-1} c_{n-1}$

Dla $n=2$:

$G_{kn} = \sum_{i=kn}^{(k+1)n-1} g_i \prod_{j=i+1}^{(k+1)n-1} p_j$ ✱

$P_k = \prod_{j=kn}^{(k+1)n-1} p_j$

$c_{kn} = \sum_{i=0}^{k-1} G_i \prod_{j=i+1}^{k-1} P_j + c_0 \prod_{j=0}^{k-1} P_j$

Dla bloku 0:

$s_0 = a_0 \oplus b_0 \oplus c_0$

$c_1 = a_0 b_0 + (a_0 + b_0) c_0$

$s_1 = a_1 \oplus b_1 \oplus c_1$

$P_0 = (a_0 + b_0)(a_1 + b_1)$

$G_0 = a_0 b_0 (a_1 + b_1) + a_1 b_1$ ~~$(a_1 + b_1)$~~