43 3-битовый S-блок

Задача. Боб проектирует блочную криптосистему, в которой используется 3-битовый S-блок, заданный многочленами Жегалкина следующим образом:

$$S(x_0, x_1, x_2) = (x_1x_2 + x_2 + x_0 + 1, x_0x_2 + x_2 + x_1 + x_0, x_0x_1 + x_2).$$

Помогите Бобу реализовать действие S-блока 7 логическими операциями из стандартного списка: $\neg$ (НЕ), $\wedge$ (И), $\vee$ (ИЛИ), $\oplus$ (исключающее ИЛИ).

Решение. Действие S-блока можно задать следующим алгоритмом:

$$\begin{aligned}
t_0 &\leftarrow \neg x_2,\\
t_1 &\leftarrow x_0 \vee x_2,\\
t_2 &\leftarrow x_0 \wedge x_1,\\
t_0 &\leftarrow t_0 \vee x_1,\\
y_1 &\leftarrow x_1 \oplus t_1,\\
y_2 &\leftarrow x_2 \oplus t_2,\\
y_0 &\leftarrow x_0 \oplus t_0.
\end{aligned}$$

S-блок является одним из 10752 криптографически оптимальных биективных 3-битовых блоков. У этих блоков нелинейность максимальна, а уравнение

$$S(x \oplus \alpha) = S(x) \oplus \beta$$

имеет не более 2 решений относительно $x \in \{0,1\}^3$ при любых ненулевых $\alpha, \beta \in \{0,1\}^3$.

Прямыми расчетами установлено (спасибо В. Семенову), что 7 операциями можно реализовать 660 оптимальных S-блоков, и ни один оптимальный блок нельзя реализовать меньшим числом операций. $\square$