Sum of Products Derivation for S-Box Functions

For each function of s returns a 2-bit number. We can develop a SOP equation for each bit separately and concatenate the outputs to get our solution for a given s function. This means that we will have 4 SOP equations for the entire s-box truth table, 2 equations for the 2 bits of s_0 and 2 equations for the 2 bits of s_1.

The S-Box Truth Table:

x_0	x_1	x_2	x_3	$s_0(x)$	$s_1(x)$
0	0	0	0	01	00
0	0	0	1	11	10
0	0	1	0	00	01
0	0	1	1	10	00
0	1	0	0	11	10
0	1	0	1	01	11
0	1	1	0	10	11
0	1	1	1	00	11
1	0	0	0	00	11
1	0	0	1	11	10
1	0	1	0	10	00
1	0	1	1	01	01
1	1	0	0	01	01
1	1	0	1	11	00
1	1	1	0	11	00
1	1	1	1	10	11

0.1 S_0 Function

First Bit:

x_0	x_1	x_2	x_3	Output	Product
0	0	0	0	0	0
0	0	0	1	1	$x_0'x_1'x_2'x_3$
0	0	1	0	0	0
0	0	1	1	1	$x_0'x_1'x_2x_3$
0	1	0	0	1	$x_0'x_1x_2'x_3'$
0	1	0	1	0	0
0	1	1	0	1	$x_0'x_1x_2x_3'$
0	1	1	1	0	0
1	0	0	0	0	0
1	0	0	1	1	$x_0x_1'x_2'x_3$
1	0	1	0	1	$x_0x_1'x_2x_3'$
1	0	1	1	0	0
1	1	0	0	0	0
1	1	0	1	1	$x_0x_1x_2'x_3$
1	1	1	0	1	$x_0x_1x_2x_3'$
1	1	1	1	1	$x_0x_1x_2x_3$

SOP Equation: Output $= x_0'x_1'x_2'x_3 + x_0'x_1'x_2x_3 + x_0'x_1x_2'x_3' + x_0'x_1x_2x_3' + x_0x_1'x_2'x_3 + x_0x_1'x_2x_3' + x_0x_1x_2'x_3 + x_0x_1x_2x_3' + x_0x_1x_2x_3$

Second Bit:

x_0	x_1	x_2	x_3	Output	Product
0	0	0	0	1	$x_0'x_1'x_2'x_3'$
0	0	0	1	1	$x_0'x_1'x_2'x_3$
0	0	1	0	0	0
0	0	1	1	0	0
0	1	0	0	1	$x_0'x_1x_2'x_3'$
0	1	0	1	1	$x_0'x_1x_2'x_3$
0	1	1	0	0	0
0	1	1	1	0	0
1	0	0	0	0	0
1	0	0	1	1	$x_0x_1'x_2'x_3$
1	0	1	0	0	0
1	0	1	1	1	$x_0x_1'x_2x_3$
1	1	0	0	1	$x_0x_1x_2'x_3'$
1	1	0	1	1	$x_0x_1x_2'x_3$
1	1	1	0	1	$x_0x_1x_2x_3'$
1	1	1	1	0	0

SOP Equation: Output $= x_0'x_1'x_2'x_3' + x_0'x_1'x_2'x_3 + x_0'x_1x_2'x_3' + x_0'x_1x_2'x_3 + x_0x_1'x_2'x_3 + x_0x_1'x_2x_3 + x_0x_1x_2'x_3' + x_0x_1x_2'x_3 + x_0x_1x_2x_3'$

0.2 S_1 Function

First Bit:

x_0	x_1	x_2	x_3	Output	Product
0	0	0	0	0	0
0	0	0	1	1	$x_0'x_1'x_2'x_3$
0	0	1	0	0	0
0	0	1	1	0	0
0	1	0	0	1	$x_0'x_1x_2'x_3'$
0	1	0	1	1	$x_0'x_1x_2'x_3$
0	1	1	0	1	$x_0'x_1x_2x_3'$
0	1	1	1	1	$x_0'x_1x_2x_3$
1	0	0	0	1	$x_0x_1'x_2'x_3'$
1	0	0	1	1	$x_0x_1'x_2'x_3$
1	0	1	0	0	0
1	0	1	1	0	0
1	1	0	0	0	0
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	1	$x_0x_1x_2x_3$

SOP Equation: Output $= x_0'x_1'x_2'x_3 + x_0'x_1x_2'x_3' + x_0'x_1x_2'x_3 + x_0'x_1x_2x_3' + x_0'x_1x_2x_3 + x_0x_1'x_2'x_3' + x_0x_1'x_2'x_3 + x_0x_1x_2x_3$

Second Bit:

x_0	x_1	x_2	x_3	Output	Product
0	0	0	0	0	0
0	0	0	1	0	0
0	0	1	0	1	$x_0'x_1'x_2x_3'$
0	0	1	1	0	0
0	1	0	0	0	0
0	1	0	1	1	$x_0'x_1x_2'x_3$
0	1	1	0	1	$x_0'x_1x_2x_3'$
0	1	1	1	1	$x_0'x_1x_2x_3$
1	0	0	0	1	$x_0x_1'x_2'x_3'$
1	0	0	1	0	0
1	0	1	0	0	0
1	0	1	1	1	$x_0x_1'x_2x_3$
1	1	0	0	1	$x_0x_1x_2'x_3'$
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	1	$x_0x_1x_2x_3$

SOP Equation: Output $= x_0'x_1'x_2x_3' + x_0'x_1x_2'x_3 + x_0'x_1x_2x_3' + x_0'x_1x_2x_3 + x_0x_1'x_2'x_3' + x_0x_1'x_2x_3 + x_0x_1x_2'x_3' + x_0x_1x_2x_3$