

[0030] At this point the expanded set known signals K' (step 204) would be as follows:

$$K' = \{x_1, x_2, x_3, x_4, t_1, t_2, t_3, t_4, y_4\} \quad \text{formula \#20}$$

[0031] Represented in binary notation the new signals are as follows:

$$t_1 = 0000111111110000 \quad \text{formula \#21}$$

$$t_2 = 0000000000110011 \quad \text{formula \#22}$$

$$t_3 = 0101010101100110 \quad \text{formula \#23}$$

$$t_4 = 0000010101100000 \quad \text{formula \#24}$$

[0032] Performing steps 206-212 for formula 2 yields the following formula for y_2 that only requires two multiplications:

$$y_2 = x_4 + (x_2 + x_1 x_3)(x_3 + x_4) \quad \text{formula \#25}$$

[0033] These steps may be repeated to obtain simplified versions of y_3 and y_4 as shown in the straight line program of formulas 26-41 below.

$$t_1 = x_1 + x_2 \quad \text{formula \#26}$$

$$t_2 = x_1 x_3 \quad \text{formula \#27}$$

$$t_3 = x_4 + t_2 \quad \text{formula \#28}$$

$$t_4 = t_1 t_3 \quad \text{formula \#29}$$

$$y_4 = x_2 + t_4 \quad \text{formula \#30}$$

$$t_5 = x_3 + x_4 \quad \text{formula \#31}$$

$$t_6 = x_2 + t_2 \quad \text{formula \#32}$$

$$t_7 = t_6 t_5 \quad \text{formula \#33}$$

$$y_2 = x_4 + t_7 \quad \text{formula \#34}$$

$$t_8 = x_3 + y_2 \quad \text{formula \#35}$$

$$t_9 = t_3 + y_2 \quad \text{formula \#36}$$

$$t_{10} = x_4 t_9 \quad \text{formula \#37}$$

$$y_1 = t_{10} + t_8 \quad \text{formula \#38}$$

$$t_{11} = t_3 + t_{10} \quad \text{formula \#39}$$

$$t_{12} = y_4 t_{11} \quad \text{formula \#40}$$

$$y_3 = t_{12} + t_1 \quad \text{formula \#41}$$

[0034] As described above, if one used formulas 1-4 for calculating y_1 - y_4 separately, 18 multiplications (AND operations) and 16 additions (XOR operations) would be required. However, using the straight line program for calculating y_1 - y_4 shown in formulas 26-41, only 5 multiplications and 11 additions are required. So, in the example of formulas 1-4 applying method 200 can yield a reduction of 13 multiplications and 5 additions.

[0035] FIG. 3 schematically illustrates the method 300 of reducing a quantity of XOR gates in greater detail. As described above, the method 300 is applied to a second portion of a combinational circuit that contains only XOR gates, also known as a linear portion of the combinational circuit. Suppose a linear portion of the combinational circuit can be represented by formulas 42-47 as shown below (step 302):

$$z_0 = w_0 + w_1 + w_2 \quad \text{formula \#42}$$

$$z_1 = w_1 + w_3 + w_4 \quad \text{formula \#43}$$

$$z_2 = w_0 + w_2 + w_3 + w_4 \quad \text{formula \#44}$$

$$z_3 = w_1 + w_2 + w_3 \quad \text{formula \#45}$$

$$z_4 = w_0 + w_1 + w_3 \quad \text{formula \#46}$$

$$z_5 = w_2 + w_3 + w_4 \quad \text{formula \#47}$$

[0036] Formulas 42-47 for z_0 - z_5 can also be represented in the form of matrix M shown in formula 48 (shown below), with each row of M representing one of the formulas for z_0 - z_5 . For example, the first row of M corresponds to z_0 , and includes a "1" for each of w_0 , w_1 and w_2 (which are all included in formula 42) and a "0" for each of w_3 and w_4 (neither of which are present in formula 42).

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{formula \#48}$$

[0037] If each of formulas z_0 - z_5 were calculated separately from scratch, 14 additions (XOR operations) would be required. One may apply the method 300 to the matrix M to see if a simplified short line program to solve for z_0 - z_5 using a reduced number of additions can be determined by using formula 49 below as a reference.

$$f(w) = Mw \quad \text{formula \#49}$$

[0038] where M is the matrix of formula 48; and

[0039] w is a value in the input vector

[0040] An input vector S is shown below in formula 50 and includes the values shown in formulas 51-55. The vector S acts as a set of signals to serve as a basis for the method 200 (step 304). As shown in formulas 51-55, each of the values w_0 - w_4 is a row of an identity matrix.

$$S = \{w_0, w_1, w_2, w_3, w_4\} \quad \text{formula \#50}$$

$$w_0 = 10000 \quad \text{formula \#51}$$

$$w_1 = 01000 \quad \text{formula \#52}$$

$$w_2 = 00100 \quad \text{formula \#53}$$

$$w_3 = 00010 \quad \text{formula \#54}$$

$$w_4 = 00001 \quad \text{formula \#55}$$

[0041] The following distance vector is then determined (step 306), as shown in formula 56:

$$D = [2 \ 2 \ 3 \ 2 \ 2 \ 3] \quad \text{formula \#56}$$

[0042] Each value in the distance vector D corresponds to a quantity of additions needed to compute a z_n value. For example, computing z_0 requires 2 additions, computing z_1 requires 2 additions, computing z_2 requires 3 additions, etc.

[0043] Two basis vectors are then chosen (step 308) whose sum, when added to the basis D minimizes the sum of the new distances. In one example $w_1 + w_3$ may be selected, as shown