This is the Title PhL 3.26.05

I had something wrong in my original set of lines resulting in (2.2.4). Here I correct them, and in the doc there is even more detail supplied. This was a non-obvious set of steps that only became non-obvious after I tried to follow them from the original doc!

The Figure 2 Iteration Equation

Figure 2 shows k registers q_1 through q_k. Construct the following polynomial:

$$q(x) = q_1 + q_2\, x + q_3\, x^2 + \ldots q_k\ x^{k-1} = \Sigma_{i=0}^{k-1}\, q_{i+1} x^i \qquad (2.2.1)$$

One can regard q(x) as a representation of the *state vector* of the shift register generator.

As shown in (1.4.1), the equation which determines the behavior of a register q_j in Figure 2 is

$$q_{j+1}(s+1) = q_j(s) - h_j\ o(s)$$

where the subscript denotes a register stage, and the argument s is a time index. We have changed this time index from n to s, because we have another use for symbol n below. We now simplify this as:

$$q'_{j+1} = q_j - h_j\ o \qquad (2.2.2)$$

where prime means one clock after no-prime. Thus, q(x) above records the register state before a clock, and q'(x) records the state after one clock,

$$q'(x) = q'_1 + q'_2\, x + q'_3\, x^2 + \ldots q'_k\ x^{k-1} = \Sigma_{i=0}^{k-1}\, q'_{i+1} x^i. \qquad (2.2.3)$$

I now claim the following is true:

$$q'(x) = x\, q(x) - o\, h(x) + i \qquad (2.2.4)$$

Proof: Start with the right side using $i = q_0$:

$$\text{RHS} = x\, q(x) - o\, h(x) + i$$

$$= x\, \Sigma_{i=0}^{k-1}\, q_{i+1} x^i - o\ \Sigma_{i=0}^{k}\, h_i x^i + q_0$$

$$= \Sigma_{i=0}^{k-1}\, q_{i+1} x^{i+1} - o\, \Sigma_{i=0}^{k}\, h_i x^i + q_0 \qquad \text{// now let } i+1 = j$$

$$= \Sigma_{j=1}^{k}\, q_j x^j - o\, \Sigma_{i=0}^{k}\, h_i x^i + q_0$$

$$= \Sigma_{j=0}^{k}\, q_j x^j - o\, \Sigma_{i=0}^{k}\, h_i x^i$$

$$= \Sigma_{i=0}^{k}\, q_i x^i - o\, \Sigma_{i=0}^{k}\, h_i x^i$$

$= \Sigma_{i=0}^{k} [q_i - oh_i] x^i$

$= \Sigma_{i=0}^{k} q'_{i+1} x^i$

$= \Sigma_{i=0}^{k-1} q'_{i+1} x^i + q'_{k+1} x^k$

$= \Sigma_{i=0}^{k-1} q'_{i+1} x$ // since $q'_{k+1} = q_{k+1}(s+1)$

$= q'(x)$