A5/1 Soft Version Explained VI

Sample of Special States - Inverse Proliferation metric

Some hints about Markovian critical processes

By Juan Chamero, juan.chamero@intag.org, as of April 2006

As we have seen we may generate a “Special States” subset out of a GF2 set of (2^n -1) members characterized by a given “pattern” within their “neighborhood” when generated by a “States Machine”. Remember that we may imagine the whole states sequence along a 2^64 – 1 bits outcome vector. At any position h we may get state S(h) by taking the bit (h) followed by the next (n-1) bits. Along this long vector we may look for some “strange” patterns, like for instance a 1 followed by 15 zeroes. If these patterns have k bits we are going to find approximately 2^(n-k) of such patterns.

If we are talking of a States Machine that runs m time steps to generate m bits outcomes we may define the pattern “neighborhood” set as the set of those states capable to generate these patterns within the m size interval. We may also use the sequence/outcome generation vector to define these neighborhoods.

Have all states within these subsets similar properties?. Well it depends of how they were generated. If generation was based on LFSR’s working linear, as if all registers worked synchronized all at a time, any state have a unique ancestry easy to find going backwards along its outcome vector. However if register activation is ruled by a non linear process any state may be the result of more than one partial states combination, and this characteristic may open more and more possible ancestors as we go upwards. If we have outcome vectors U1, U2 and U3, for each register, of dimensions 2^19-1, 2^22-1, and 2^23-1 respectively, any state at time step (t) could be defined by the following relation:

$$S(t) = S1(i+t)OS2(j+t)OS3(k+t)$$

Where S1(i), S2(j), S3(k) are the initial partial states at time t=0, located at positions [i j k] within their respective outcome vectors U1, U2, and U3 that is we obtain S by concatenating (O) three partial states. As time advances working within linearity, the above relation holds true for any t. On the contrary, working within non linearity t advance does not mean registers advance or virtually pointers advance along either component of the triplet [I j k]. For this reason for any state S(t) we may find instead

$$S(t) = S1(i+t1)OS2(j+t2)OS3(k+t3)$$

Where at time (t) the triplet [t1 t2 t3] corresponding to triplet [i j k] at time “distance” t is of probabilistic nature with a mean of ¾ of t. Ignoring t, going backwards from any state defined by its 64 bits content (19 in R1, 22 in R2 and 23 in R3), and also ignoring the initial positioning triplet [i j k], has the form of a Markovian process. Each state content may have from none to four possible ancestors with an average of 1 so it’s perfectly possible to find sequences of let’s say 1,2 ancestors along 100 levels which becomes 13,780 possible ancestors!.

We may then define a sort of Reverse Proliferation factor just counting the potential ancestors within certain “bandwidths” measured in levels of backwards trees. This metric is then useful to differentiate Special States in at least two families: Prolific and Non Prolific. Prolific states are those that could be find going forward as “descendants” within the neighborhood of “hidden” states as explained above.

Below we listed a sample of 1000 states whose contents are expressed in hexadecimal. Under X it’s listed the amount of possible ancestors within time steps 100 and 277.

Nr.	EE	[R1 R2 R3]	X	Level attained
EE2		[edfb 7b3c3 2684df]	2302	277
EE18		[edfb 1971bf 2c47a0]	3015	277
EE22		[edfb 1e437f 28e740]	3835	277
EE50		[edfb 17f7a0 9037f]	4960	277
EE67		[1dbf7 1f1787 1b83fe]	7024	277
EE71		[1dbf7 167cdf 1c03c3]	1434	277
EE106		[1dbf7 1f7fa0 2037f]	2140	277
EE111		[1dbf7 1f0740 de3fe]	4550	277
EE130		[3b7ef 19f337 1887d0]	3164	277
EE131		[3b7ef df4df 1807d0]	4081	277
EE132		[3b7ef df4df 1807a0]	1933	277
EE154		[3b7ef c9fd0 2710e6]	1570	277
EE157		[3b7ef cbfd0 2421bf]	869	277
EE187		[76fdf 17d1bf 1207d0]	5400	277
EE191		[76fdf d7bfe 8429e]	730	277
EE196		[76fdf affe8 20437f]	893	277
EE233		[5bf7c df1e1 837f]	1232	277
EE237		[5bf7c 2f0e6 3707f4]	1809	277
EE240		[5bf7c 7e1cc 30770e]	1804	277
EE242		[5bf7c 1fee66 801cc]	1174	277
EE264		[5bf7c 1bfff4 10278]	3981	277
EE265		[5bf7c 1bfff4 200e6]	1111	277
EE316		[37ef9 17ffa0 101bf]	1221	277
EE337		[6fdf3 1cf1bf e17d0]	2891	277
EE353		[6fdf3 ef5ff c17a0]	4289	277
EE361		[6fdf3 1ef3fe 82740]	2092	277
EE363		[6fdf3 7fff4 1037f]	4110	277
EE366		[6fdf3 7ffe8 401cc]	1241	277
EE379		[6fdf3 7f7d0 403fe]	4328	277
EE381		[6fdf3 7e7a0 5e1bf]	7511	277
EE382		[6fdf3 7ffa0 2037f]	2122	277
EE394		[5fbe7 1fff87 411e1]	578	277
EE418		[5fbe7 1ef37f 381740]	900	277
EE448		[5fbe7 1f67d0 204df]	2553	277
EE460		[5fbe7 1fe7a0 403fe]	1604	277
EE468		[5fbe7 1fc680 1037f]	759	277
EE471		[3f7cf 1be3c3 18070e]	2576	277
EE472		[3f7cf 1fe3c3 101bf]	2627	277
EE476		[3f7cf f9787 403fe]	2232	277
EE502		[3f7cf ef3fe 1837d0]	3512	277
EE508		[3f7cf fe7e8 1037f]	6199	277
EE516		[3f7cf fe7a0 2037f]	442	277
EE520		[3f7cf fe740 2037f]	2500	277

EE576	[7ef9f f8501 433fe]	2140	277
EE581	[7df3e e761c 2403fe]	5606	277
EE630	[77cfa df1bf 2e67d0]	2334	277
EE677	[6f9f4 1e03fe 8c740]	1278	277
EE685	[6f9f4 79ff4 804df]	551	277
EE700	[6f9f4 7cfa0 204df]	849	277
EE703	[6f9f4 7cfa0 1f6ff]	692	277
EE709	[6f9f4 79740 3e3fe]	867	277
EE727	[5f3e9 1bf4df 17a0]	3309	277
EE736	[5f3e9 1df1bf 38d740]	2395	277
EE747	[5f3e9 1df5ff 127d0]	3307	277
EE761	[5f3e9 1f97f4 4037f]	614	277
EE769	[5f3e9 1f8fe8 3e3fe]	2763	277
EE775	[5f3e9 1f17d0 7c3fe]	2294	277
EE776	[5f3e9 1f97a0 614df]	3685	277
EE780	[5f3e9 1f97a0 7c5ff]	2700	277
EE782	[5f3e9 1f9740 204df]	1468	277
EE815	[3e7d3 1df1bf 11a680]	1260	277
EE826	[3e7d3 823fe 1b4787]	2365	277
EE839	[3e7d3 f17d0 3e3fe]	2374	277
EE872	[7cfa7 1df1bf 34501]	826	277
EE873	[7cfa7 9f37f 148740]	1525	277
EE876	[7cfa7 1df37f 10404]	1466	277
EE887	[7cfa7 1c13fe 36501]	2976	277
EE888	[7cfa7 1c13fe 6c404]	5314	277
EE890	[7cfa7 cd7a0 1011bf]	4642	277
EE926	[79f4f 82ffd 2d8202]	1868	277
EE933	[79f4f b680 2411bf]	2067	277
EE934	[79f4f 88680 27d3fe]	1814	277
EE936	[79f4f cb501 8237f]	1247	277
EE987	[4fa7d 1f7ffd 280012]	3121	277