M. F. Ezerman, A. A. Fahreza and J. Szmidt

On cross-join method for de Bruijn sequences and Zech logarithma

Recently several papers have apeared on construction of de Bruijn sequences from some classes of Linear Feedback Shift Registers (*LFSRs*). The authors have used the method of joining cycles generated by some reducible *LFSRs*. In [1] we proved that having one de Bruijn sequence of a given order one can construct all de Bruijn sequences of that order by repeated application of the cross-join pairs method. In [2] we presented a method to find cross-join pairs of states by calculating Zech logarithms in Galois fields. This enables us to construct feedback Boolean functions of Nonlinear Feedback Shift Registers (*NFSRs*) of maximum period up to the order of n = 430 and for any primitive trinomial. In the case of primitive trinomials we can calculate the cross-join pairs by hand.

In [3] the Freyers' formula was presented, which is a new analytic tool in the theory of *NFSRs*. Combining the Freyers' formula and our cross-join theorem [1] we proposed in [2] an algorithm to generate the feedback Boolean functions of all de Bruijn sequences of given order n starting from one m-sequence of order n. The algorithm has a finite number of stages and at each stage we generate a fixed number of feedback Boolean functions. To illustrate the process we obtain the following sequences of numbers of generated Boolean functions: for $n = 5$,

$$(1, 35, 273, 715, 715, 273, 35, 1),$$

summing to $2048 = 2^{11}$, and for $n = 6$,

$$(1, 155, 6293, 105183, 876525, 4032015, 10855425, 17678835,$$

$$17678835, 10855425, 4032015, 876525, 105183, 6293, 155, 1),$$

summing to $67108864 = 2^{26}$, which is the total number of de Bruijn sequences of order 6. The above numbers of sequences were obtained from the Freyers' formula and confirmed experimentally. Here 35 is the number of cross-join pairs for an m-sequence of order 5, 273 is the number of new feedback Boolean functions of *NFSRs* obtained after second application of the cross-join method, etc. After application of the cross-join method seven times we produce all feedback Boolean functions of de Bruijn sequences of order 5.

References

[1] J. Mykkeltveit, J. Szmidt. *On cross joining de Bruijn sequences.* Contemporary Mathematics, 2015, vol.63, pp.335-346.

[2] J. Szmidt. Nonlinear Feedback Shift Registers and Zech Logarithms. ArXiv e-prints, October 2017.

[3] D. Coppersmith, R. C. Rhoades, J. M. Vanderkam. *Counting de Bruijn Sequences as Perturbation of Linear Recursions.* arXiv: 1705.07835v [math.CO] 22 May 2017.