

# My favorite proof on Boolean functions: The proof by Mykkeltveit of Golomb's conjecture for the deBruijn graph

Tor Helleseth

University of Bergen, Norway

In his book "Shift Register Sequences" in 1967, Solomon W. Golomb conjectured that the number of cycles generated by any arbitrary binary recurrence relation of a Boolean function does not exceed the number of cycles provided by the pure cycling register. In the 1970s I started as a master student supervised by Ernst S. Selmer at the Department of Mathematics, University of Bergen, Norway. The research group in Bergen at this time was led by Ernst S. Selmer and was particularly interested in the conjecture due to Solomon W. Golomb. The PhD student in our group, Johannes Mykkeltveit, worked very hard on this problem for a full year. Finally he solved the problem finding an extremely beautiful and elegant proof.

The paper was published in 1972 in Journal of Combinatorial Theory. The paper was only 6 pages long including introduction and background definitions. I followed closely the progress of the work by Mykkeltveit on this problem. I was fascinated by the incredible elegant and surprising proof that even today is the most elegant proof I have ever seen in my career.

In this talk I will give the history of the problem and its unusual simple and fascinating proof.