# Feedback with Carry Shift Registers and Bent Sequences

1/C Charles Celerier, Honors Pure Mathematics, Spring 2012

Professor David Joyner, Department of Mathematics

## Abstract

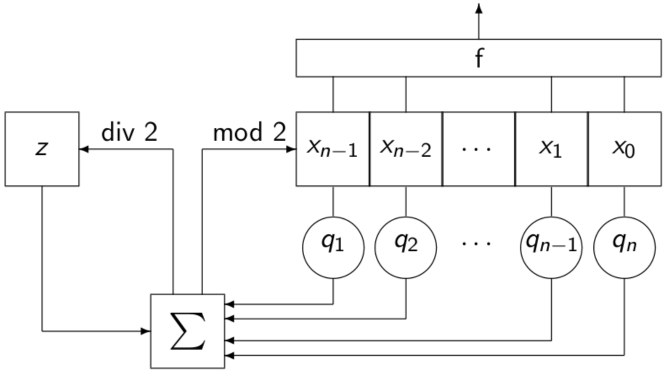
A stream cipher uses pseudorandom sequences to mimic the security of a one-time pad. This project investigated how bent functions can be used to generate *f*-filtered bent sequences with large 2-adic valuation. Rearrangements of these sequences could be effective for filtering the states of feedback with carry shift registers (FCSRs) in stream ciphers. The non-linearity of *f*-filtered bent sequences could provide resistance for FCSR-based stream ciphers in register synthesis attacks.

## Results

It turns out that the 2-adic integer valuation of an *f*-filtered bent sequence using a Boolean function from the Maiorana-McFarland class is

$$2^{n/2} + 2^{\overline{\pi}(0)}$$

In addition to this result, Sage code was written to demonstrate examples for the project. This code will soon be submitted for inclusion in the next Sage release.



FCSRs, like the one pictured above, can be filtered with a bent function *f* which produces different types of bent sequences depending on the periodicity of the states in the register.

## Relevance

There is a wide range of military and civilian applications that use pseudorandom sequences in stream ciphers to secure communications. Having the capability to analyze different types of pseudorandom sequences enables cryptographers to create more secure designs for the stream ciphers they make. Also, the lines of code written in Sage will be a contribution to the growing library of classes in Sage.