Sidon-Mengen, APN-Funktionen und ihre Zusammenhänge

Eine Sidon-Menge S ist eine Teilmenge von $\mathbb{F}_2^n$ derart, dass die Summen $s+s'$ mit $s, s' \in S$ alle verschieden sind. Ursprünglich wurden solche Mengen ($\approx$ 1930) nur in den ganzen Zahlen betrachtet (Simon Sidon).

In der letzten Dekade wurden solche Mengen dann von mehreren Autoren wiederentdeckt (z.B. Carlet, Mesnager, Picek, Thornburgh, Redman, Rose, Walker, Nagy). Einer der Gründe dafür ist vermutlich, dass der Graph einer APN (almost perfect nonlinear) Funktion ein Beispiel einer Sidon-Menge ist: APN Funktionen sind Abbildungen $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mit der Eigenschaft, dass $f(x+a)+f(x) = b$ für jedes $a \neq 0$ genau 0 oder 2 Lösungen hat. Die Motivation, solche Abbildungen zu betrachten, kommt aus der Kryptographie, und solche Abbildungen werden seit vielen Jahren intensiv studiert.

In meinem Vortrag werde ich den Zusammenhang zwischen Sidon und APN erläutern und einige spannende offene Fragen diskutieren, insbesondere die nach der maximalen Größe einer Sidon-Menge.

Dem Vortrag liegen Arbeiten mit meinem Doktoranden Ingo Czerwinski zugrunde.