

---

**ANDREA BURGESS**, University of New Brunswick Saint John  
*Cyclic circular external difference families*

A  $(v, m, \ell, 1)$ -Circular External Difference Family (CEDF) is an  $m$ -sequence  $(A_1, \dots, A_m)$  of  $\ell$ -subsets of an additive group  $G$  of order  $v$  such that the multiset of all differences  $a - a'$ , with  $(a, a') \in A_{i+1 \pmod m} \times A_i$  for some  $i \in \mathbb{Z}_m$ , is equal to  $G \setminus \{0\}$ . When  $G = \mathbb{Z}_v$ , we speak of a *cyclic CEDF*. CEDFs are a variation of External Difference Families, and have been recently introduced as a tool to construct non-malleable threshold schemes.

Necessarily, if a  $(v, m, \ell, 1)$ -CEDF exists, then  $v = m\ell^2 + 1$ . It is known that an  $(m\ell^2 + 1, m, \ell, 1)$ -CEDF over the cyclic group exists whenever the number of subsets  $m$  is even, while there cannot exist a cyclic CEDF for  $m$  and  $\ell$  both odd. In this talk, we consider the existence of cyclic CEDFs in the case that  $m$  is odd and  $\ell$  is even. In particular, we construct a cyclic  $(m\ell^2 + 1, m, \ell, 1)$ -CEDF for any odd  $m > 1$  when  $\ell = 2$ , and for any even  $\ell \geq 2$  when  $m = 3$ .

This is joint work with Francesca Merola and Tommaso Traetta.