The weight spectrum of the Reed-Muller codes $RM(m-5,m)$

Claude Carlet,
Universities of Bergen, Norway and Paris 8, France

The weight spectra (i.e. the lists of all possible weights) of the Reed-Muller codes $RM(r,m)$, of length 2^m and order r, are unknown for $r \in \{3,\ldots,m-5\}$ (and m large enough). Those of $RM(m-4,m)$ and $RM(m-3,m)$ have been determined very recently (but not the weight distributions, giving the number of codewords of each weight, which seem out of reach). We determine the weight spectrum of $RM(m-5,m)$ for every $m \geq 10$. We proceed by first determining the weights in $RM(5,10)$. To do this, we construct functions whose weights are in the set $\{62,74,78,82,86,90\}$, and functions whose weights are all the integers between 94 and $2^9-2=510$ that are congruent with 2 modulo 4 (those weights that are divisible by 4 are easier to determine and they are indeed known). This allows us to determine completely the weight spectrum, thanks to the well-known result due to Kasami, Tokura and Azumi, which precisely determines those codeword weights in Reed-Muller codes which lie between the minimum distance d and 2.5 times d, and thanks to the fact the weight spectrum is symmetric with respect to 2^9. Then we use this particular weight spectrum for determining that of $RM(m-5,m)$, by an induction on m. We check that a recent conjecture (in which we correct a misprint) on the weight spectrum of $RM(m-c,m)$ is verified for $c=5$, and we study the difficulties of trying to extend the results to $c \geq 6$.

To appear in IEEE Transactions on Information Theory.