

Known power permutations x^d with the highest known nonlinearity over \mathbb{F}_{2^n} , $n = 2t$

Exponents d	Conditions	Proven
$2^t + 1$	$\gcd(i, n) = 2, t$ odd	[3]
$2^{2^i} - 2^i + 1$	$\gcd(i, n) = 2, t$ odd	[4]
$2^{n-1} - 1$		[5]
$2^t + 2^{\frac{t+1}{2}} + 1$	t odd	[1]
$2^t + 2^{t-1} + 1$	t odd	[1]
$2^t + 2^{\frac{t}{2}} + 1$	$t \equiv 2 \pmod{4}$	[2]
$\sum_{k=0}^t 2^{ik}$	$\gcd(i, n) = 1, t$ even	[2, 6]

References

- [1] Thomas W Cusick and Hans Dobbertin. Some new three-valued crosscorrelation functions for binary m-sequences. *IEEE Transactions on Information Theory*, 42(4):1238–1240, 1996.
- [2] Hans Dobbertin. One-to-one highly nonlinear power functions on gf (2 n). *Applicable Algebra in Engineering, Communication and Computing*, 9(2):139–152, 1998.
- [3] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE transactions on Information Theory*, 14(1):154–156, 1968.
- [4] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information and Control*, 18(4):369–394, 1971.
- [5] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonal of the extended quadratic binary goppa codes. *IEEE transactions on information theory*, 36(3):686–692, 1990.
- [6] Yoji Niho. Multi-valued cross-correlation functions between two maximal linear recursive sequences. Technical report, UNIVERSITY OF SOUTHERN CALIFORNIA LOS ANGELES ELECTRONIC SCIENCES LAB, 1972.