CLAUDE GRAVEL, Tutte Institute for Mathematics and Computing

Permutations with one cycle of maximal length, and output bits of maximal algebraic degree

Let $n \geq 3$ be an odd positive integer. We study a subset $A \subset S_{2^n}$ for which every element has four properties. Properties are: (I) no more than $2n$ bits are needed to describe a permutation in A, (II) the algebraic degree of all the n output boolean functions is $n-1$; an element of A takes $(a_0, \ldots, a_{n-1}) = a \in \{0,1\}^n$ as an input and produces an output $(\varphi_0(a), \ldots, \varphi_{n-1}(a)) \in \{0,1\}^n$ where φ_j is a boolean function for $j \in \{0, \ldots, n-1\}$, (III) every permutation in A has one cycle of length 2^n, and (IV) the expected number of terms (products of the a_i's) of the boolean functions φ_j for $j \in \{0, \ldots, n-1\}$ is $O(2^{n-1})$. Every element in A is associated to some irreducible polynomial $Q \in \mathbb{Z}_2[X]$ such that $\deg(Q) = n$, and to an exponent $d \in \{n, \ldots, 2^n - 2\}$; the output of an element $a \in \{0,1\}^n$ is computed by (1) the input a be encoded as $P_a(X) = a_0 + \ldots + a_{n-1}X^{n-1}$, (2) let $R_{a,0}(X) = P_a(X)$ and for $\ell \in \{1, \ldots, n\}$, let $R_{a,\ell}(X) = (R_{a,\ell-1}(X) + X^d)^{-2^{\ell-1}} \mod Q(X)$, and (3) output the coefficients of $R_{a,n-1}(X)$. The cardinality of A is smaller than $\frac{1}{n}\sum_{d|n} 2^d \mu(\frac{n}{d})$ which is the number of irreducible polynomials of degree n. For a given n, characterizing polynomials that yields the four properties is my main goal together with proving the fourth property. Properties one and two are proven mathematically. Properties three and four are supported by symbolic computation with some yet unfigured steps for the proof of property three. I wish eventually to show that the ratio of the cardinality of A and $\frac{1}{n}\sum_{d|n} 2^d \mu(\frac{n}{d}) \in O\big(\frac{2^n}{n}\big)$ is *not* zero asymptotically with respect to n.