Permutations with special properties

Claude Grave

Let $n \geq 3$ be an odd positive integer. Based upon the properties of $\mathbb{F}_{2^n}$, I study the construction of a subset A of the symmetric group S_{2^n}. Every element in A has four interesting properties. The first property states that no more than $2n$ bits are needed to describe a permutation in A. The second property states that the algebraic degree of all the n output boolean functions is $n-1$; an element of A takes $(a_0, \ldots, a_{n-1}) = a \in \mathbb{Z}_2^n$ as an input and produces an output $(\varphi_0(a), \ldots, \varphi_{n-1}(a)) \in \mathbb{Z}_2^n$ where φ_j is a boolean function for $j \in \{0, \ldots, n-1\}$. The third property states that every permutation in A has one cycle of length 2^n. The fourth property states 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 carefully selected irreducible polynomial $Q \in \mathbb{Z}_2[X]$ such that $\deg(Q) = n-1$, and to a polynomial $P \in \mathbb{Z}_2[X] \backslash \{0\}$. The polynomial P is called the perturbation polynomial. Any element $a \in \mathbb{Z}_2^n$ is canonically associated to $P_a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$. A permutation $F \in A$ such that $F(a) = b$ is defined through the sequence $a^{(j)} \in \mathbb{Z}_2^n$ for $j = 0, \ldots, n$ such that (1) $P_{a^{(0)}}(X) = (P_a(X) + P(X))^{-2^0}$, (2) $P_{a^{(j)}}(X) = (P_{a^{(j-1)}}(X) + P(X))^{-2^{j-1}}$ for $j \in \{1, \ldots, n\}$, and (3) $b = a^{(n)}$. The set A *may* be connected to the set of primitive irreducible polynomials. 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. If characterizing such irreducible polynomials seems hard, then I wish eventually to show that the ratio of the cardinality of A and $\frac{1}{n} \sum_{d|n} 2^d \mu(\frac{n}{d}) \in O\left(\frac{2^n}{n}\right)$ is *not* zero asymptotically with respect to n or at least tends to zero *very* slowly for all practical purposes.