Boolean functions with multiple special properties

Claude Gravel[1], **Daniel Panario**[2], **David Thomson**[2]

In this work, we construct a subset $T_{2^n} \subset S_{2^n}$, with S_{2^n} the symmetric group on 2^n letters, for which all members satisfy several properties simultaneously. Elements in T_{2^n} are *unicyclic strong permutations* and are built using facts from finite fields.

Let $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n$, and for $\sigma \in T_{2^n}$ let $\sigma(a) = (\varphi_0(a), \ldots, \varphi_{n-1}(a))$, where φ_j is the jth coordinate function of σ, $0 \leq j < n$. Then

1. every boolean function φ_j has algebraic degree equal to $n-1$,
2. the number of terms of φ_j in the a_i's is $2^{n-1} \pm C$ with C a small constant,
3. the permutation σ has only one cycle of length 2^n,
4. the differential uniformity of σ is low, typically 4 or 6.

Here, the first two properties are proven, and the final two properties are based on substantial empirical evidence.

Let $Q \in \mathbb{F}_2[X]$ be an irreducible polynomial and let $P \in \mathbb{F}_2[X]/(Q(X))$ be a fixed non-constant polynomial. We construct a global permutation σ as the composition of permutations $\sigma = \sigma_{n-1} \circ \sigma_{n-2} \circ \cdots \circ \sigma_0$. Each σ_k can be thought of as a round of a symmetric cipher. For $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n$, let $P_a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$. Then each σ_k is given by the polynomial

$$P_{\sigma_k(a)}(X) \equiv \big(P_a(X) + P(X)\big)^{-2^k} \pmod{Q}. \tag{1}$$

We call P from Equation (1) the *perturbation polynomial*. Moreover each σ_k^{-1} has polynomial representation

$$P_{\sigma_k^{-1}(a)}(X) \equiv \big(P_a^{-2^{n-k}}(X) + P(X)\big) \pmod{Q}.$$

We obtain our results, both explicit and empirical, with the fixed perturbation $P(X) = 1 + X^{n-1}$.

The high algebraic degree and the large number of terms in each coordinate function (Properties 1. and 2. above) ensure that solving $b = \sigma(a)$ without knowledge of P and Q is hard using algebraic methods.

Empirically for n even, σ contains many small cycles and for n odd σ contains only few long cycles. For some choices of Q of degree $n = 15, 17, 19$, we also compute the differential uniformity of σ, which for a given permutation f is given by $\max_{a \in \mathbb{F}_{2^n} \setminus \{0\}, b \in \mathbb{F}_{2^n}} |x \in \mathbb{F}_{2^n} : f(x+a) - f(x) = b|$. In these cases, we found no differential uniformity greater than 6. We further conjecture that for large values of n, the number of difference equations having 3 pairs of solutions is negligible.

Empirically, given a perturbation polynomial P, the fraction of irreducible polynomials yielding unicyclic strong permutations does not tend to 0, and seems to vary according to choice of P.

[1]Département d'informatique et de recherche opérationnelle, Université de Montréal
[2]School of Mathematics and Statistics, Carleton University