Linear characters and boolean circuits

Laszlo Egri

Let F be a field and F^* be its multiplicative group (which is always cyclic) with generator g. We are interested in the vector space $V = \{f : (F^*)^n \to F\}$. Linear characters are functions of the form $P(x_1, ..., x_n) = g^{c_1 x_1 + ... + c_n x_n}$. We can show that the linear characters form a basis for V e.g. using a Vandermonde matrix argument. This basis turns out to have important applications in proving lower bounds for circuits, e.g. no subexponential size circuit in which there is a layer of MOD-q gates followed by a MOD-p gate can compute the AND function. We also studied relationships between the support of a function f (the number of inputs for which f is non-zero) in V and the number of Ps needed to express f.