Simple Affine Extractors using Dimension Expansion

Ariel Gabizon

October 5, 2009

Abstract

Let $\mathbb{F}_q$ be the field of q elements. An (n,k)-*affine extractor* is a mapping $D : \mathbb{F}_q^n \to \{0,1\}$ such that for any k-dimensional affine subspace $X \subseteq \mathbb{F}_q^n$, $D(x)$ is an almost unbiased bit when x is chosen uniformly from X. Loosely speaking, the problem of explicitly constructing affine extractors gets harder as q gets smaller and easier as k gets larger. This is reflected in previous results: When q is 'large enough', specifically $q = \Omega(n^2)$, Gabizon and Raz construct affine extractors for any $k \geq 1$. In the 'hardest case', i.e. when $q = 2$, Bourgain constructs affine extractors for $k \geq \delta n$ for any constant (and even slightly sub-constant) $\delta > 0$. Our main result is the following: Fix any $k \geq 2$ and let $d = 5n/k$. Then whenever $q > 2 \cdot d^2$ and $p = char(\mathbb{F}_q) > d$, we give an explicit (n,k)-affine extractor. For example, when $k = \delta n$ for constant $\delta > 0$, we get an extractor for a field of constant size $\Omega(\left(\frac{1}{\delta}\right)^2)$. Thus our result may be viewed as a 'field-size/dimension' tradeoff for affine extractors. Although for large k we are not able to improve (or even match) the previous result of Bourgain, our construction and proof have the advantage of being very simple: Assume n is prime and d is odd, and fix any non-trivial linear map $T : \mathbb{F}_q^n \mapsto \mathbb{F}_q$. Define $QR : \mathbb{F}_q \mapsto \{0,1\}$ by $QR(x) = 1$ if and only if x is a quadratic residue. Then, the function $D : \mathbb{F}_q^n \mapsto \{0,1\}$ defined by $D(x) \triangleq QR(T(x^d))$ is an (n,k)-affine extractor.

Our proof uses a result of Heur, Leung and Xiang giving a lower bound on the dimension of products of subspaces.

Joint work with Matt DeVos