Electronic Colloquium on Computational Complexity, Report No. 63 (2009)

Simple Affine Extractors using Dimension Expansion

Matt DeVos*Ariel Gabizon†

July 29, 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 [3] construct affine extractors for any $k \geq 1$. In the 'hardest case', i.e. when $q = 2$, Bourgain [2] 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 $\Omega((\frac{1}{\delta})^2)$. 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 [2], 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 [4] giving a lower bound on the dimension of products of subspaces.

1 Introduction

In this paper we consider the problem of explicitly constructing *affine extractors*: Color a vector space , say with 2 colors, such that every large enough affine subspace has roughly the same number of points of each color. Let us define this formally. First, we say that a distribution P on $\{0,1\}$ is ϵ-*close uniform* if $|\Pr(P=1) - 1/2| \leq \epsilon$.

*Department of Mathematics, Simon Fraser University, Vancouver, Canada. mdevos@sfu.ca

†Department of Computing Science, Simon Fraser University, Vancouver, Canada. ariel.gabizon@gmail.com.

ISSN 1433-8092

Definition 1 (Affine extractor). *Fix integers $1 \leq k \leq n$ and a field $\mathbb{F}_q$. A function $D : \mathbb{F}_q^n \mapsto \{0,1\}$ is an (n,k)-affine extractor with error ϵ, if for any k-dimensional affine subspace $X \subseteq \mathbb{F}_q^n$ $D(X)$ is ϵ-close to the uniform.*

Remark 1.1. *Affine extractors are usually defined as outputting* many *bits, and indeed one important goal is constructing affine extractors with large output length. However, as in this paper our new results are not related to the number of output bits, for simplicity we define affine extractors as boolean functions (see also Remark 5.1).*

Affine extractors can be motivated in at least two ways. First, as a derandomization question: A central goal in the field of derandomization and pseudorandomness is to explicitly construct objects that have properties a random function would have with high probability; and indeed, a random function is with high probability a (n,k)-affine extractor, for example when $k = O(\log n)$ for any $q \geq 2$. A second motivation comes from the field of extractors: Consider a scenario when a computation requires a random string but has access only to a 'weak random source'. An extractor is a function that converts 'weak randomness' to a string that is statistically close to a true random string. There are many ways to formally define a weak random source. One way to define it would be a uniform distribution on an unknown k-dimensional subspace. In such a case, an affine extractor would enable us to produce random bits from such a weak random source. See the survey of Shaltiel[7] for a review of this broad field.

1.1 Previous Work and Our Result

Intuitively, constructing affine extractors gets harder as the underlying field size q gets smaller and easier as the dimension k of the subspace gets larger. Gabizon and Raz [3] construct affine extractors for $q = \Omega(n^2)$ for any $k \geq 1$. When $q = 2$, Bourgain [2] constructs affine extractors for $k \geq \delta n$ for any constant (and even slightly sub-constant) $\delta > 0$ (see also the simplification and improvement by Yehudayoff [9]).

Ben-Sasson and Kopparty [1] recently managed to break the 'linear-entropy barrier' for $q = 2$, and construct weaker objects called affine dispersers for $k = 6 \cdot n^{4/5}$ over $\mathbb{F}_2$. It seems that the results of [1] can easily be adapted using Weil's theorem (see Section 2) to give affine extractors for $k, q = O(n^{4/5})$. Our main result may be viewed as a 'field-size/dimension' tradeoff. The larger the dimension of the subspace, the smaller field size we can work with.

Theorem 1. *Fix a field $\mathbb{F}_q$ of characteristic p and integers $2 \leq k \leq n$ and $n \geq 25$. Let $s = \frac{6n}{5 \cdot (k-1)} + 2$. Assume that $p > s$ and $q > 2 \cdot s^2$. There is an explicit (n,k)-affine extractor $D : \mathbb{F}_q^n \mapsto \{0,1\}$ with error $\epsilon = s/\sqrt{q}$. In particular, when $p > (5n/k)$ and $q \geq 2 \cdot (5n/k)^2$ the theorem holds and we get an extractor with error $\epsilon = O((n/k)/\sqrt{q})$.*

One interesting instantiation of Theorem 1 is when $k = \delta \cdot n$ for constant $\delta > 0$. In this case, we get an affine extractor for a field of constant size $q = \Omega((1/\delta)^2)$. Again, this does not match the result of Bourgain[2]. For the range $\omega(1) < k < n/\log n$ no other result to our knowledge[1] gives explicit affine extractors for field size $q = \Omega((n/k)^2)$. However, even for ranges of parameters where

[1] It seems that an unpublished result of the second author gives smaller field size for $k = o(\sqrt{n})$.

we do not improve or match previous results, our construction and proof have the advantage of being very simple. An annoying drawback is the requirement for large characteristic. Basically, this is to due to the fact that many multinomial coefficients become zero in fields of small characteristic.

2 Overview of the Proof

A central component in our proof is a theorem of Weil[8, 6] on the number of points on curves over finite fields and, more specifically, its applications to character sums. We roughly state the corollary of Weil's theorem that we will use (see Subsection 3.1 for a precise formulation): Let $f(t_1, \ldots, t_k)$ be a non-constant polynomial of degree d over $\mathbb{F}_q$ where both d and q are odd. Then, when choosing $(t_1, \ldots, t_k)$ uniformly at random, the probability that $f(t_1, \ldots, t_k)$ is a quadratic residue in $\mathbb{F}_q$ is close to $1/2$ provided q is a bit larger than d^2. For simplicity, we forget about the requirement of d being odd for the rest of this discussion. Thus, Weil's theorem reduces the task of constructing an affine extractor to that of constructing a low-degree polynomial $f : \mathbb{F}_q^n \mapsto \mathbb{F}_q$ of that is non-constant on any k-dimensional subspace: Once we have such a polynomial, we simply output 0 or 1 according to whether $f(x_1, \ldots, x_n)$ is a quadratic residue in $\mathbb{F}_q$, and we are guaranteed that this is an almost unbiased bit. More specifically, if we manage to construct a polynomial of degree d that is non-constant on affine subspaces of dimension k, we get an affine extractor for field size roughly d^2. Gabizon and Raz [3] used the polynomial $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^i$. It is not hard to show that this polynomial will be non-constant on any 1-dimensional affine subspace. Thus, they get an $(n, 1)$-affine extractor for $q = \Omega(n^2)$. In this paper we show how to construct a polynomial f of degree roughly n/k that is non-constant on any k-dimensional affine subspace. Our construction is as follows. Let d be an integer larger than $\frac{n}{k-1}$. Let $T : \mathbb{F}_q^n \mapsto \mathbb{F}_q$ be a non-trivial $\mathbb{F}_q$-linear function. Given a vector $x \in \mathbb{F}_q^n$, we think of x as an element in the field $\mathbb{F}_{q^n}$. Define $f(x) \triangleq T(x^d)$ (It is easy to see that when thinking of f as a multivariate polynomial over $\mathbb{F}_q$ it indeed has degree d). We want to show that f is non-constant when restricted to k-dimensional subspaces. Fix an affine subspace $X \subseteq \mathbb{F}_q^n$ whose linear component has basis $a_1, \ldots, a_k \in \mathbb{F}_q^n$. When restricting f to X it can be seen that the coefficients of the degree d monomials are $\mathbb{F}_q$-scalar multiples of the T-image of the monomials of degree d in $a_1, \ldots, a_k$. If we could show that the monomials of total degree d in $a_1, \ldots, a_k$ span $\mathbb{F}_q^n$ over $\mathbb{F}_q$, it would follow that one of them must have a non-zero image under T, and therefore the restriction of f to X is non-constant of degree d. This will indeed follow from a theorem of Heur, Leung and Xiang [4] about 'products of subspaces'. From [4] we will deduce that when $a_1, \ldots, a_k$ are linearly independent, the monomials of total degree d in them span[2] a subspace of dimension at least $(k-1) \cdot d + 1$, or span the whole space. The theorem of [4] is actually more general, and we will give a self-contained proof of the specific result we need (see Subsection 3.2).

[2] Actually, this will be true when n is prime

3 Preliminaries

Notation: Let $f : \mathbb{F}_q^n \mapsto \mathbb{F}_q$ be a function. For an affine subspace $X \subseteq \mathbb{F}_q^n$ defined by basis vectors $a_1, \ldots, a_k \subseteq \mathbb{F}_q^n$ and translation vector $b \in \mathbb{F}_q^n$, we denote f restricted to X by $f|_X$. That is, for $t_1, \ldots, t_k \in \mathbb{F}_q$, $f|_X(t_1, \ldots, t_k) \triangleq f(a_1 \cdot t_1 + \ldots + a_k \cdot t_k + b)$. For a set Ω, we denote by U_Ω the uniform distribution on Ω. For a function $f : \Omega \mapsto \Gamma$ and a distribution P on Ω, we denote by $f(P)$ the distribution induced on Γ by sampling from P and applying f. Given a vector, $x \in \mathbb{F}_q^n$ we will often view x as an element in $\mathbb{F}_{q^n}$ and use multiplication in this field.

3.1 Characters of Finite Fields and Weil's Theorem

Loosely speaking, given an abelian group G, a *character* on G is a map from G to complex roots of unity that preserves the group action. The characters of a finite field are the characters of the additive and multiplicative[3] groups of the field. We will only use multiplicative characters.

Definition 2 (Multiplicative character)**.** *A function $\chi : \mathbb{F}_q \to \mathbb{C}$ is a multiplicative character of $\mathbb{F}_q$ if $|\chi(a)| = 1$ for every $a \in \mathbb{F}_q^*$ and $\chi(0) = 0$ and*

$$\chi(ab) = \chi(a)\chi(b)$$

for every $a, b \in \mathbb{F}_q$. The order of χ is the smallest integer m such that $(\chi(a))^m = 1$ for every $a \in \mathbb{F}_q^*$.

For our extractor we will use the 'quadratic residue' character (that exists whenever the field has odd characteristic).

Definition 3 (Quadratic residue character)**.** *Let $q = p^l$ for some integer l and odd prime p. We define the multiplicative character $\chi_1 : \mathbb{F}_q \to \{-1, 0, 1\}$ to be 1 for a non-zero quadratic residue, -1 for a quadratic non-residue, and 0 on 0. More concisely,*

$$\chi_1(a) = a^{\frac{q-1}{2}}.$$

We define the function $QR : \mathbb{F}_q \to \{0, 1\}$ by $QR(a) = 1$ if $\chi_1(a) = -1$, and $QR(a) = 0$ otherwise. That is, $QR(a) = 1$ for quadratic non-residues and 0 otherwise.

A very useful theorem of Weil [8] state that for any low degree polynomial f that is not of a certain restricted form, the values of a field character 'cancel out' over the range of f (when viewed as a multi-set). We state this theorem for multiplicative characters.

Theorem 1. *[6][Theorem $2C'$, page 43] Let χ be a multiplicative character of $\mathbb{F}_q$ of order $m > 1$. Let $f(t)$ be a non-constant polynomial in $\mathbb{F}_q[t]$ of degree d. Suppose that $f(t)$ is not of the form $c \cdot g(t)^m$ for any $c \in \mathbb{F}_q$ and $g(t) \in \mathbb{F}_q[t]$. Then*

$$\left| \sum_{t \in \mathbb{F}_q} \chi(f(t)) \right| \leq d \cdot q^{1/2}.$$

[3] A character χ of $\mathbb{F}_q^*$ is extended to 0 by $\chi(0) = 0$.

For the case of a field character of order 2, Weil's theorems actually show that the character is an 'extractor' for distributions of the form $f(U_{\mathbb{F}_q})$ for a low odd degree polynomial f . We formalize this in the following Corollary (see [3] for a proof).

Corollary 3.1. *Let $q = p^l$ for some integer l and odd prime p. Let $f(t) \in \mathbb{F}_q[t]$ be a non-constant polynomial of degree m that is not a square multiple in $\mathbb{F}_q[t]$. Then $QR(f(U_{\mathbb{F}_q}))$ is ϵ-close to uniform for $\epsilon = \frac{d}{\sqrt{q}}$.*

A similar statement can now be shown for multivariate low degree polynomials.

Lemma 3.2. *Let $q = p^l$ for some integer l and odd prime p. Let $f(t_1, \ldots, t_k) \in \mathbb{F}_q[t_1, \ldots, t_k]$ be a non-constant polynomial of total degree d for odd $d < q$. Then $QR(f(U_{\mathbb{F}_q^k}))$ is ϵ-close to uniform for $\epsilon = \frac{d}{\sqrt{q}}$.*

Proof. We note first that there must be an $a \in \mathbb{F}_q^n$ such that the univariate 'line restriction' polynomial $f_a(t) \triangleq f(a \cdot t, \ldots, a \cdot t)$ has degree (exactly) d: The coefficient of t^d in f_a is $f^d(a)$ where f^d is the d-homogenous part of f, i.e., the sum of monomials of degree exactly d in f, and by the Schwartz-Zippel lemma as $d < q$, there is an a such that $f^d(a) \neq 0$. Furthermore, for such $a \in \mathbb{F}_q^n$, for all $b \in \mathbb{F}_q^n$ $f_{a,b}(t) \triangleq f(a \cdot t + b)$ has degree exactly d - as terms including b will have degree smaller than d and cannot cancel out a d'th power of t. As the distribution $f(U_{\mathbb{F}_q^k})$ is a convex combination of distributions $f_{a,b}(U_{\mathbb{F}_q})$ for different 'shifts' $b \in \mathbb{F}_q^n$ the claim now follows from Corollary 3.1. □

3.2 Dimension Expansion of Products of Subspaces

For $\mathbb{F}_q$-linear subspaces $A, B \subseteq \mathbb{F}_q^n$ we define the 'product' subspace $A \cdot B \triangleq \text{span}(a \cdot b | a \in A, b \in B)$. Note that if $a_1, \ldots, a_l$ and $b_1, \ldots, b_k$ are bases for A and B respectively, then $A \cdot B = \text{span}(a_i \cdot b_j | 1 \leq i \leq l, 1 \leq j \leq k)$. Similarly, for an element $a \in \mathbb{F}_q^n$ and linear subspace $B \subseteq \mathbb{F}_q^n$ we denote by $a \cdot B$ the set $\{a \cdot b | b \in B\}$ (which is also a linear subspace of the same dimension as multiplication by a is a non-singular $\mathbb{F}_q$-linear transformation).

The following theorem of Hou, Leung and Xiang[4] generalizes a famous Theorem of Kneser (see [4] for background). It gives a lower bound on the dimension of a product of subspaces. We state the theorem for completeness but we will only use the corollary below.

Theorem 2 ([4] Theorem 2.4)**.** *Let $E \subset K$ be fields and let A and B be finite-dimensional E-linear subspaces of positive dimension. Suppose that every algebraic element in K is seperable over E. Then*

$$dim_E(A \cdot B) \geq dim_E(A) + dim_E(B) - dim_E(H(A \cdot B))$$

where $H(A \cdot B) = \{x \in K | x \cdot A \cdot B \subseteq A \cdot B\}$ is the stabilizer of $A \cdot B$ in K.

Corollary 3.3. *Let $\mathbb{F}_q$ be any field, and let n be prime. Let A and B be $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ having positive dimension. Then*

$$dim(A \cdot B) \geq \min\{n, dim(A) + dim(B) - 1\}$$

We give a self-contained proof of the corollary based on [4].

Proof. We note first that we can assume that $1 \in B$: Otherwise, choose $b \in B$ and let $B' = \{b^{-1} \cdot B\}$. Then $1 \in B'$, $dim(B') = dim(B)$ and $dim(A \cdot B') = dim(A \cdot B)$. We prove the claim by induction on $dim(A)$. If $dim(A) = 1$ then $dim(A \cdot B) = dim(B)$ and the claim holds. Now let $dim(A) = l$ and let $\{a_1, \ldots, a_l\}$ be a basis for A. Assume without loss of generality that $a_l \notin \mathbb{F}_q$ (only one of the a_i's can be in $\mathbb{F}_q$). Let $A^{l-1} = \text{span}(a_1, \ldots, a_{l-1})$. From the induction hypothesis $dim(A^{l-1} \cdot B) \geq \min\{n, dim(A) + dim(B) - 2\}$. Note that $A \cdot B = \text{span}(A^{l-1} \cdot B, a_l \cdot B)$. If $a_l \cdot B \nsubseteq A^{l-1} \cdot B$ then $dim(A \cdot B) > dim(A^{l-1} \cdot B)$ and we are done. Assume now that $a_l \cdot B \subseteq A^{l-1} \cdot B$. As $1 \in B$, a_l can be expressed as an $\mathbb{F}_q$-linear combination of the elements of $A^{l-1} \cdot B$. Therefore, any power of a_l can be expressed as an $\mathbb{F}_q$-linear combination of the elements of $A^{l-1} \cdot B$, and thus $A^{l-1} \cdot B$ contains the field generated over $\mathbb{F}_q$ by a_l. As n is prime this must be $\mathbb{F}_{q^n}$ and so $dim(A \cdot B) = n$. □

4 The Main Construction

Theorem 3. *Fix a field $\mathbb{F}_q$ of characteristic p and integers $2 \leq k \leq n$ such that n is prime. Fix any integer d with $\frac{n}{k-1} \leq d < p$. Let $T : \mathbb{F}_q^n \mapsto \mathbb{F}_q$ be a non-trivial $\mathbb{F}_q$-linear mapping. Then the polynomial $f : \mathbb{F}_q^n \mapsto \mathbb{F}_q$ defined by $f(x) = T(x^d)$ is non-constant on all affine subspaces of dimension k. Furthermore, for any k-dimensional affine subspace X, $f|_X$ has total degree* exactly *d.*

Proof. Fix any k-dimensional affine subspace X. Then

$$f|_X(t_1, \ldots, t_k) = T((a_1 \cdot t_1 + \ldots + a_k \cdot t_k + b)^d).$$

Fix non-negative integers $i_1, \ldots, i_k$ with $i_1 + \ldots + i_k = d$. Note that the coefficient of $t_1^{i_1} \cdots t_k^{i_k}$ in $f|_X$ is

$$T\left(\frac{d!}{i_1! \cdots i_k!} \cdot a_1^{i_1} \cdots a_k^{i_k}\right) = \frac{d!}{i_1! \cdots i_k!} \cdot T(a_1^{i_1} \cdots a_k^{i_k}),$$

where the equality follows as T is $\mathbb{F}_q$-linear. We would like to prove that one of these coefficients is non-zero. As $p > d$, the above coefficient is non-zero if and only if

$$T(a_1^{i_1} \cdots a_k^{i_k}) \neq 0.$$

We will prove that the set of monomials in the a_i's of total degree d span $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Thus, one of these monomials must be mapped by T to a non-zero value in $\mathbb{F}_q$, and therefore $f|_X$ is non-constant of total degree d. For this purpose, for $1 \leq j \leq d$ define $A_j \subseteq \mathbb{F}_q^n$ to be the subspace spanned by the set of monomials in the a_i's of total degree exactly j. That is

$$A_j \triangleq \text{span}(a_1^{i_1} \cdots a_k^{i_k} | i_1 + \ldots + i_k = j).$$

We will prove by induction that $dim(A_j) \geq \min\{n, (k-1) \cdot j + 1\}$ (from which the theorem will follow): For $j = 1$, $A_1 = \text{span}(a_1, \ldots, a_k)$ and as the a_i's are linearly independent the claim

follows. Now assume the claim for $j-1$. Note that $A_j = A_{j-1} \cdot A_1$. Thus, using Corollary 3.3,

$$dim(A_j) \geq \min\{n, (k-1)\cdot(j-1)+1+k-1\} = \min\{n, (k-1)\cdot j+1\}.$$

□

5 Our Affine Extractor

We restate and prove our main theorem.

Theorem 1. *Fix a field $\mathbb{F}_q$ of characteristic p and integers $2 \leq k \leq n$ and $n \geq 25$. Let $s = \frac{6n}{5\cdot(k-1)} + 2$. Assume that $p > s$ and $q > 2 \cdot s^2$. There is an explicit (n,k)-affine extractor $D : \mathbb{F}_q^n \mapsto \{0,1\}$ with error $\epsilon = s/\sqrt{q}$.*

Proof. Choose a prime $n \leq n' \leq (6/5)\cdot n$ (which always exists for $n \geq 25$ according to Nagura's improvement of the Bertrand-Cebychev Theorem[5]) and pad $x \in \mathbb{F}_q^n$ with zeros to get a vector in $\mathbb{F}_q^{n'}$. Let $f : \mathbb{F}_q^{n'} \mapsto \mathbb{F}_q$ be the polynomial in Theorem 3 where we take d to be the smallet odd integer that is at least $\frac{n'}{k-1}$. Let $D : \mathbb{F}_q^n \mapsto \{0,1\}$ be defined as $D(x) \triangleq QR(f(x))$. From Theorem 3 we know that for any k-dimensional affine subspace $X \subseteq \mathbb{F}_q^{n'}$, $f|_X$ is non-constant of degree exactly d. Therefore, for any such X from Lemma 3.2 we know that $D(X)$ is ϵ-close to uniform for $\epsilon = (d/\sqrt{q}) \leq (s/\sqrt{q})$ and the theorem follows. □

Remark 5.1. *Using the methods of Gabizon and Raz[3] we could extend our extractor to extract $(k-1)\log q$ bits at the expense of requiring a field of size $q = \Omega((n/k)^c)$, for a universal constant $c \sim 40$.*

Acknowledgements

We thank Luis Goddyn for a very helpful conversation.

References

[1] E. Ben-Sasson and S. Kopparty. Affine dispersers from subspace polynomials. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 65–74, 2009.

[2] J. Bourgain. On the construction of affine extractors. *Geometric & Functional Analysis*, 17 Number 1:33–57, 2007.

[3] A. Gabizon and R. Raz. Deterministic extractors for affine sources over large fields. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 407–418. IEEE Computer Society, 2005.

[4] X. Hour, K.H. Leung, and Q. Xiang. A generalization of an addition theorem of kneser. *Journal of Number Theory*, 97:1–9, 2002.

[5] J. Nagura. On the interval containing at least one prime number. *Proceedings of the Japan Academy*, 28:177–181, 1952.

[6] W. M. Schmidt. *Equations over Finite Fields: An Elementary Approach*, volume 536. Springer-Verlag, Lecture Notes in Mathematics, 1976.

[7] R. Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[8] A. Weil. On some exponential sums. In *Proc. Nat. Acad. Sci. USA*, volume 34, pages 204–207, 1948.

[9] A. Yehudayoff. Affine extractors over prime fields. *Manuscript*, 2009.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de