From affine to two-source extractors via approximate duality

Eli Ben-Sasson Noga Zewi

Computer Science Department
Technion — Israel Institute of Technology

May 2011

Approximate duality and discrepancy

- Given $A, B \subset \mathbb{F}_2^n$ let their *duality constant* (or *discrepancy*) be

$$D(A,B) = \left| \mathbb{E}_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right|, \text{ where } \langle a,b \rangle = \sum_{i=1}^{n} a_i b_i.$$

Approximate duality and discrepancy

- Given $A, B \subset \mathbb{F}_2^n$ let their *duality constant* (or *discrepancy*) be

$$D(A,B) = \left| \mathbb{E}_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right|, \text{ where } \langle a,b \rangle = \sum_{i=1}^{n} a_i b_i.$$

- Clearly $D(A,B) = 1$ iff $A \subseteq b + B^{\perp}$ for some $b \in \mathbb{F}_2^n$.

Approximate duality and discrepancy

- Given $A, B \subset \mathbb{F}_2^n$ let their *duality constant* (or *discrepancy*) be

$$D(A,B) = \left| \mathbb{E}_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right|, \text{ where } \langle a,b \rangle = \sum_{i=1}^{n} a_i b_i.$$

- Clearly $D(A,B) = 1$ iff $A \subseteq b + B^{\perp}$ for some $b \in \mathbb{F}_2^n$.
- Question: What if $D(A,B) > 0.99$?

Approximate duality and discrepancy

- Given $A, B \subset \mathbb{F}_2^n$ let their *duality constant* (or *discrepancy*) be

$$D(A,B) = \left| \mathbb{E}_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right|, \text{ where } \langle a,b \rangle = \sum_{i=1}^{n} a_i b_i.$$

- Clearly $D(A,B) = 1$ iff $A \subseteq b + B^{\perp}$ for some $b \in \mathbb{F}_2^n$.
- Question: What if $D(A,B) > 0.99$?
- Answers (this talk):

Approximate duality and discrepancy

- Given $A, B \subset \mathbb{F}_2^n$ let their *duality constant* (or *discrepancy*) be

$$D(A,B) = \left| \mathbb{E}_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right|, \text{ where } \langle a,b \rangle = \sum_{i=1}^{n} a_i b_i.$$

- Clearly $D(A,B) = 1$ iff $A \subseteq b + B^{\perp}$ for some $b \in \mathbb{F}_2^n$.
- Question: What if $D(A,B) > 0.99$?
- Answers (this talk):
  1. There exist "large" subsets A', B' of A, B such that $D(A',B') = 1$.

Approximate duality and discrepancy

- Given $A, B \subset \mathbb{F}_2^n$ let their *duality constant* (or *discrepancy*) be

$$D(A,B) = \left| \mathbb{E}_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right|, \text{ where } \langle a,b \rangle = \sum_{i=1}^{n} a_i b_i.$$

- Clearly $D(A,B) = 1$ iff $A \subseteq b + B^{\perp}$ for some $b \in \mathbb{F}_2^n$.
- Question: What if $D(A,B) > 0.99$?
- Answers (this talk):
  1. There exist "large" subsets A', B' of A, B such that $D(A',B') = 1$.
  2. Assuming the polynomial Freiman-Ruzsa conjecture (PFR), A', B' as above exist even when $D(A,B) > 2^{-\Omega(n)}$.

One main point

Theorem (Discrepancy in matrices of small rank)

Assuming PFR, for every $\alpha, \delta > 0$ exists $\gamma > 0$ such that:
If $M \in \mathbb{F}_2^{N \times N}$ has $\mathbb{F}_2$-rank at most $\frac{\log N}{\alpha}$ and discrepancy greater than $2^{-\gamma n}$ then M contains a large monochromatic rectangle $M[S, T], |S|, |T| \geq N^{1-\frac{\delta}{\alpha}}$.

One main point

Theorem (Discrepancy in matrices of small rank)

Assuming PFR, for every $\alpha, \delta > 0$ exists $\gamma > 0$ such that:
If $M \in \mathbb{F}_2^{N \times N}$ has $\mathbb{F}_2$-rank at most $\frac{\log N}{\alpha}$ and discrepancy greater than $2^{-\gamma n}$ then M contains a large monochromatic rectangle
$M[S, T], |S|, |T| \geq N^{1-\frac{\delta}{\alpha}}$.

Conjecture (Polynomial Freiman-Ruzsa (PFR))

Let $\sigma_2(A) = |A + A|/|A|$ where $A + A = \{a + a' \mid a, a' \in A\}$. There exists a constant c such that for every $A \subset \mathbb{F}_2^n$ we have:
$\exists A' \subset A, |A'| \geq |A|/\sigma_2(A)^c$ *such that* $|A'|/|\mathrm{span(A')}| \geq \sigma_2(\mathrm{A})^{-\mathrm{c}}$.

Affine and two-source dispersers/extractors

Definition (Affine Extractor)

is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that for all affine sources $X \subseteq \mathbb{F}_2^n$ of min-entropy rate $\frac{\dim(X)}{n}$ at least ρ,

$$\|f(X) - U_m\|_\infty \leq \epsilon.$$

Definition (Two-source extractor)

is a function $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that for all pairs of independent sources $X, Y \subseteq \mathbb{F}_2^n$ of min-entropy rate at least ρ,

$$\|f(X, Y) - U_m\|_\infty \leq \epsilon.$$

Affine and two-source dispersers/extractors

Definition (Affine Disperser)

is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that for all affine sources $X \subseteq \mathbb{F}_2^n$ of min-entropy rate $\frac{\dim(X)}{n}$ at least ρ,

$$|f(X)| > 1.$$

Definition (Two-source disperser)

is a function $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ such that for all pairs of independent sources $X, Y \subseteq \mathbb{F}_2^n$ of min-entropy rate at least ρ,

$$|f(X, Y)| > 1.$$

Three main points

- "Good" affine extractors (small rate and error) can be converted in a black-box manner into "good" two-source dispersers (small rate).
- Two-source dispersers of low $\mathbb{F}_2$-rank are extractors with bounded error.
- Under the polynomial Freiman-Ruzsa conjecture (PFR), extractor error is exponentially small.

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2} + \epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2} - O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2} - \epsilon_0$	exponentially small

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

- Affine

Reference	rate	error
Folklore (prob. method)	$O(\frac{\log n}{n})$	random function

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

- Affine

Reference	rate	error
Folklore (prob. method)	$O(\frac{\log n}{n})$	random function
BHRVW '01	$\frac{1}{2}+\epsilon$	exponentially small

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

- Affine

Reference	rate	error
Folklore (prob. method)	$O(\frac{\log n}{n})$	random function
BHRVW '01	$\frac{1}{2}+\epsilon$	exponentially small
BKSSW '05	ϵ	dispersers

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

- Affine

Reference	rate	error
Folklore (prob. method)	$O(\frac{\log n}{n})$	random function
BHRVW '01	$\frac{1}{2}+\epsilon$	exponentially small
BKSSW '05	ϵ	dispersers
Bourgain '07	ϵ	exponentially small

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

- Affine

Reference	rate	error
Folklore (prob. method)	$O(\frac{\log n}{n})$	random function
BHRVW '01	$\frac{1}{2}+\epsilon$	exponentially small
BKSSW '05	ϵ	dispersers
Bourgain '07	ϵ	exponentially small
Yehudayoff '09, Li '10	$\epsilon/\log\log n$	exponentially small

Previous constructions

- Two-source

Reference	rate	error
Erdös '47 (prob. method)	$O(\frac{\log n}{n})$	disperser
Chor, Goldreich '88	$\frac{1}{2}+\epsilon$	exponentially small
Pudlák, Rödl '04	$\frac{1}{2}-O(\frac{1}{\sqrt{n}})$	dispersers
Bourgain '05	$\frac{1}{2}-\epsilon_0$	exponentially small
BKSSW '05	ϵ	disperser
BRSW '06	$n^{1-\epsilon}$	disperser

- Affine

Reference	rate	error
Folklore (prob. method)	$O(\frac{\log n}{n})$	random function
BHRVW '01	$\frac{1}{2}+\epsilon$	exponentially small
BKSSW '05	ϵ	dispersers
Bourgain '07	ϵ	exponentially small
Yehudayoff '09, Li '10	$\epsilon/\log\log n$	exponentially small
Ben-Sasson, Kopparty '09	$n^{-3/5}$	disperser

A pair of two-source extractors

Given $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (presumably, an affine extractor)

- The *concatenated* two-source extractor $C : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ is defined by

$$C(x, y) = \langle x \circ f(x), y \circ f(y) \rangle.$$

A pair of two-source extractors

Given $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (presumably, an affine extractor)

- The *concatenated* two-source extractor $C : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ is defined by
$$C(x, y) = \langle x \circ f(x), y \circ f(y) \rangle.$$
- Let $F : \mathbb{F}_2^{n-m} \to \mathbb{F}_2^n$ be injective on $f^{(-1)}(z)$ for some $z \in \mathbb{F}_2^m$. The *preimage* two-source extractor $P : \mathbb{F}_2^{n-m} \times \mathbb{F}_2^{n-m} \to \mathbb{F}_2$ is defined by
$$P(x, y) = \langle F(x), F(y) \rangle.$$

Main results — From affine to two-source

- Assume $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an affine extractor for min entropy rate ρ with ℓ_∞-error at most 2^{-m}.

Main results — From affine to two-source

- Assume $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an affine extractor for min entropy rate ρ with ℓ_∞-error at most 2^{-m}.
- The *loss rate* is defined as $\lambda = 1 - \frac{m}{\rho n}$.
- Smaller λ means more entropy is recovered by extractor.

Main results — From affine to two-source

- Assume $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an affine extractor for min entropy rate ρ with ℓ_∞-error at most 2^{-m}.
- The *loss rate* is defined as $\lambda = 1 - \frac{m}{\rho n}$.
- Smaller λ means more entropy is recovered by extractor.
- Bourgain '07: Extractors for any $\rho > 0$, achieving $\lambda_\rho < 1$.

Main results — From affine to two-source

- Assume $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an affine extractor for min entropy rate ρ with ℓ_∞-error at most 2^{-m}.
- The *loss rate* is defined as $\lambda = 1 - \frac{m}{\rho n}$.
- Smaller λ means more entropy is recovered by extractor.
- Bourgain '07: Extractors for any $\rho > 0$, achieving $\lambda_\rho < 1$.

Theorem (From affine extractors to two-source disperser)

- *The concatenated construction is a two-source disperser for min-entropy rate ρ' satisfying (i) $\rho' < 1/2$ when $\rho < 1/2$, and (ii) $\rho' \xrightarrow{\lambda \to 0} 2/5$.*
- *The pre-image construction is a two-source disperser for rate $\rho' = \frac{\lambda}{1+\lambda} \xrightarrow{\lambda \to 0} 0$, as long as $\rho \leq 1/2$.*

Main results — rank, discrepancy, approximate duality

- Given two-source function $g : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ let $\mathrm{rank}_2(g)$ be the $\mathbb{F}_2$-rank of $M_g \in \mathbb{F}_2^{\mathbb{F}_2^n \times \mathbb{F}_2^n}$ where $M_g[x, y] = g(x, y)$.
- We have $0 \leq \mathrm{rank}_2(g) \leq 2^n$.
- Rank of previously shown constructions is linear in n.

Theorem (Low-rank dispersers are extractors)

Assume g is a two-source disperser of min-entropy rate ρ and rank $O(n)$.

- *g is a two-source extractor for min-entropy rate $\rho + \epsilon$ and error strictly less than $\frac{1}{2}$.*
- *Assuming PFR, g is a two-source extractor for min-entropy rate $\rho + \epsilon$ and error $2^{-\Omega(\epsilon n)}$.*

Main results — rank, discrepancy, approximate duality

- The *doubling constant* of $A \subset \mathbb{F}_2^n$ is $\sigma_2(A) = |2A|/|A|$, where $2A = \{a + a' \mid a, a' \in A\}$.
- We have $1 \leq \sigma_2(A) \leq |A|$ and $\sigma_2(A) = 1$ iff A is a linear space.

Main results — rank, discrepancy, approximate duality

- The *doubling constant* of $A \subset \mathbb{F}_2^n$ is $\sigma_2(A) = |2A|/|A|$, where $2A = \{a + a' \mid a, a' \in A\}$.
- We have $1 \leq \sigma_2(A) \leq |A|$ and $\sigma_2(A) = 1$ iff A is a linear space.

Theorem (Freiman-Ruzsa)

If $\sigma_2(A)$ is small with respect to A then A contains a "large" subset that is a "large" fraction of a linear space.

- "Large" means exponential in $\sigma_2(A)$.
- PFR conjecture: "Large" means polynomial in $\sigma_2(A)$.

On PFR and approximate duality

Conjecture (PFR)

There exists a constant c such that every $A \subseteq \mathbb{F}_2^n$ *contains a subset* A' *of size* $|A|/(\sigma_2(A))^c$ *such that* $|A'|/|\mathrm{span}(\mathrm{A}')| \geq \sigma_2(\mathrm{A})^{\mathrm{c}}$.

On PFR and approximate duality

Conjecture (PFR)

There exists a constant c such that every $A \subseteq \mathbb{F}_2^n$ contains a subset A' of size $|A|/(\sigma_2(A))^c$ such that $|A'|/|\mathrm{span}(A')| \geq \sigma_2(A)^c$.

Conjecture (Approximate duality (ADC))

If $A, B \subset \mathbb{F}_2^n$ are of size $2^{\Omega(n)}$ and have large discrepancy:

$$D(A,B) := \left| E_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right| \geq \mu.$$

Then A, B contain large subsets that are contained in affine shifts of strictly dual sets.

On PFR and approximate duality

Conjecture (PFR)

There exists a constant c such that every $A \subseteq \mathbb{F}_2^n$ contains a subset A' of size $|A|/(\sigma_2(A))^c$ such that $|A'|/|\mathrm{span}(A')| \geq \sigma_2(A)^c$.

Conjecture (Approximate duality (ADC))

If $A, B \subset \mathbb{F}_2^n$ are of size $2^{\Omega(n)}$ and have large discrepancy:

$$D(A,B) := \left| E_{a \in A, b \in B} \left[(-1)^{\langle a,b \rangle} \right] \right| \geq \mu.$$

Then A, B contain large subsets that are contained in affine shifts of strictly dual sets.

Theorem (PFR vs. ADC)

PFR implies ADC and ADC implies a weak (though unproven) form of PFR.

On PFR and ADC

Theorem (Approximate duality for nearly-dual sets)

For $\delta > 0$ exists $\epsilon > 0$ s.t. for $A, B \subset \mathbb{F}_2^n$ with $D(A,B) \geq 1-\epsilon$ there exist $A' \subset A, |A'| \geq |A|/2$ and $B' \subset B, |B'| \geq 2^{-\delta n}|B|$ with $D(A',B') = 1$.

On PFR and ADC

Theorem (Approximate duality for nearly-dual sets)

For $\delta > 0$ exists $\epsilon > 0$ s.t. for $A, B \subset \mathbb{F}_2^n$ with $D(A,B) \geq 1-\epsilon$ there exist $A' \subset A, |A'| \geq |A|/2$ and $B' \subset B, |B'| \geq 2^{-\delta n}|B|$ with $D(A',B') = 1$.

Theorem (Discrepancy in matrices of small rank)

Assuming PFR, for every $\alpha, \delta > 0$ exists $\gamma > 0$ such that the following holds. If $M \in \mathbb{F}_2^{N \times N}$ has rank at most $\frac{\log N}{\alpha}$ and discrepancy greater than $2^{-\gamma n}$ then M contains a large monochromatic rectangle $M[S,T], |S|, |T| \geq N^{1-\frac{\delta}{\alpha}}$.

From affine to two-source extractors

Theorem (From affine extractors to two-source disperser)

- *The concatenated construction is a two-source disperser for min-entropy rate* $\rho' \overset{\lambda \to 0}{\longrightarrow} 2/5$.
- *If* $\rho = 1/2$ *the pre-image construction is a two-source disperser for rate* $\rho' = \frac{\lambda}{1+\lambda} \overset{\lambda \to 0}{\longrightarrow} 0$.

From affine to two-source extractors

Theorem (From affine extractors to two-source disperser)

- *The concatenated construction is a two-source disperser for min-entropy rate* $\rho' \overset{\lambda \to 0}{\longrightarrow} 2/5$.
- *If* $\rho = 1/2$ *the pre-image construction is a two-source disperser for rate* $\rho' = \frac{\lambda}{1+\lambda} \overset{\lambda \to 0}{\longrightarrow} 0$.

Theorem (Low-rank dispersers are extractors)

Assume g *is a two-source disperser of min-entropy rate* ρ *and rank* $O(n)$.

- g *is a two-source disperser for min-entropy rate* $\rho + \epsilon$ *and error strictly less than* $\frac{1}{2}$.
- *Assuming PFR,* g *is a two-source extractor for min-entropy rate* $\rho + \epsilon$ *and error* $2^{-\Omega(\epsilon n)}$.

Approximate duality

Theorem (Approximate duality for nearly-dual sets)

For $\delta > 0$ exists $\epsilon > 0$ s.t. for $A, B \subset \mathbb{F}_2^n$ with $D(A, B) \geq 1 - \epsilon$ there exist $A' \subset A, |A'| \geq |A|/2$ and $B' \subset B, |B'| \geq 2^{-\delta n}|B|$ with $D(A', B') = 1$.

Approximate duality

Theorem (Approximate duality for nearly-dual sets)

For $\delta > 0$ exists $\epsilon > 0$ s.t. for $A, B \subset \mathbb{F}_2^n$ with $D(A,B) \geq 1 - \epsilon$ there exist $A' \subset A, |A'| \geq |A|/2$ and $B' \subset B, |B'| \geq 2^{-\delta n}|B|$ with $D(A',B') = 1$.

Theorem (PFR implies ADC)

Assuming PFR, for every $\alpha, \delta > 0$ exists $\gamma > 0$ s.t. the following holds. If $A, B \subset \mathbb{F}_2^n$ are of size at least $2^{\alpha n}$ and have nontrivial discrepancy $D(A,B) \geq 2^{-\gamma n}$, then there exist $A' \subset A, B' \subset B$ of size $2^{(\alpha-\delta)n}$ such that $D(A',B') = 1$.