Open Problems in Analysis of Boolean Functions

Compiled for the Simons Symposium, February 5–11, 2012

For notation and definitions, see e.g.
http://analysisofbooleanfunctions.org
Correlation Bounds for Polynomials

**Statement:** Find an explicit (i.e., in NP) function \( f : \mathbb{F}_2^n \to \mathbb{F}_2 \) such that we have the correlation bound \( |E[(-1)^{f(x), p(x)}]| \leq 1/n \) for every \( \mathbb{F}_2 \)-polynomial \( p : \mathbb{F}_2^n \to \mathbb{F}_2 \) of degree at most \( \log_2 n \).

**Source:** Folklore dating back to [Raz87, Smo87]

**Remarks:**
- The problem appears to be open even with correlation bound \( 1/\sqrt{n} \) replacing \( 1/n \).
- Define the mod\(_3\) function to be 1 if and only if the number of 1’s in its input is congruent to 1 modulo 3. Smolensky [Smo87] showed that mod\(_3\) has correlation at most 2/3 with every \( \mathbb{F}_2 \)-polynomial of degree at most \( c\sqrt{n} \) (where \( c > 0 \) is an absolute constant). For related bounds using his techniques, there seems to be a barrier to obtaining correlation \( o(1/\sqrt{n}) \).
- Babai, Nisan, and Szegedy [BNS92] implicitly showed a function in \( \mathbb{P} \) which has correlation at most \( \exp(-n^{O(1)}) \) with any \( \mathbb{F}_2 \)-polynomial of degree at most \( 0.99 \log_2 n \); see also [VW08]. Bourgain [Bou05] (see also [GRS05]) showed a similar (slightly worse) result for the mod\(_3\) function.

**Tomaszewski’s Conjecture**

**Statement:** Let \( a \in \mathbb{R}^n \) have \( \|a\|_2 = 1 \). Then \( \Pr_{x \sim \{-1,1\}^n}[|\langle a, x \rangle| \leq 1] \geq 1/2 \).

**Source:** Question attributed to Tomaszewski in [Guy89]

**Remarks:**
- The bound of 1/2 would be sharp in light of \( a = (1/\sqrt{2}, 1/\sqrt{2}) \).
- Holman and Kleitman [HK92] proved the lower bound 3/8. In fact they proved \( \Pr_{x \sim \{-1,1\}^n}[|\langle a, x \rangle| < 1] \geq 3/8 \) (assuming \( a_i \neq \pm 1 \) for all \( i \)), which is sharp in light of \( a = (1/2, 1/2, 1/2, 1/2) \).

**Talagrand’s “Convolution with a Biased Coin” Conjecture**

**Statement:** Let \( f : \{-1,1\}^n \to \mathbb{R}^{\geq 0} \) have \( \mathbb{E}[f] = 1 \). Fix any \( 0 < \rho < 1 \). Then \( \Pr[T_{\rho f} \geq t] < o(1/t) \).

**Source:** [Tal89]

**Remarks:**
- Talagrand in fact suggests the bound \( O(t/\sqrt{\log t}) \).
- Talagrand offers a $1000 prize for proving this.
- Even the “special case” when \( f \)'s domain is \( \mathbb{R}^n \) with Gaussian measure is open. In this Gaussian setting, Ball, Barthe, Bednorz, Oleszkiewicz,
and Wolff [BBB’10] have shown the upper bound $O(\frac{1}{t\sqrt{\log t}})$ for $n = 1$
and the bound $O(\frac{\log \log t}{t\sqrt{\log t}})$ for any fixed constant dimension.

**Sensitivity versus Block Sensitivity**

*Statement:* For any $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ it holds that $\deg(f) \leq \text{poly}(\text{sens}[f])$, where sens[f] is the (maximum) sensitivity, $\max_x |\{i \in [n] : f(x) \neq f(x^{\oplus i})\}|$.

*Source:* [CFGS88, Sze89, GL92, NS94]

*Remarks:*
- As the title suggests, it is more usual to state this as $\text{bs}[f] \leq \text{poly}(\text{sens}[f])$, where bs[f] is the “block sensitivity”. However the version with degree is equally old, and in any case the problems are equivalent since it is known that bs[f] and deg(f) are polynomially related.
- The best known gap is quadratic ([CFGS88, GL92]) and it is suggested ([GL92]) that this may be the worst possible.

**Gotsman–Linial Conjecture**

*Statement:* Among degree-$k$ polynomial threshold functions $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$, the one with maximal total influence is the symmetric one $f(x) = \text{sgn}(p(x_1 + \cdots + x_n))$, where $p$ is a degree-$k$ univariate polynomial which alternates sign on the $k + 1$ values of $x_1 + \cdots + x_n$ closest to 0.

*Source:* [GL94]

*Remarks:*
- The case $k = 1$ is easy.
- Slightly weaker version: degree-$k$ PTFs have total influence $O(k) \cdot \sqrt{n}$.
- Even weaker version: degree-$k$ PTFs have total influence $O(k^2) \cdot \sqrt{n}$.
- The weaker versions are open even in the case $k = 2$. The $k = 2$ case may be related to the following old conjecture of Holzman: If $g : \{-1, 1\}^n \rightarrow \mathbb{R}$ has degree 2 (for $n$ even), then $g$ has at most $\binom{n}{n/2}$ local strict minima.
- It is known that bounding total influence by $c(k) \cdot \sqrt{n}$ is equivalent to bounding $\delta$-noise sensitivity by $O(c(k)) \cdot \sqrt{\delta}$.
- The “Gaussian special case” was solved by Kane [Kan09].
- The best upper bounds known are $2n^{1-1/2^k}$ and $2^{O(k)}\cdot n^{1-1/O(k)}$ [DHK+10].

**Polynomial Freiman–Ruzsa Conjecture (in the $\mathbb{F}_2^n$ setting)**

*Statement:* Suppose $\varnothing \neq A \subseteq \mathbb{F}_2^n$ satisfies $|A + A| \leq C|A|$. Then $A$ can be covered by the union of poly($C$) affine subspaces, each of cardinality at most $|A|$.

*Source:* Attributed to Marton in [Ruz93]; for the $\mathbb{F}_2^n$ version, see e.g. [Gre05b]

*Remarks:*
• The following conjecture is known to be equivalent: Suppose \( f : \mathbb{F}_2^n \to \mathbb{F}_2^n \) satisfies \( \text{Pr}_{x,y}[f(x)+f(y)=f(x+y)] \geq \epsilon \), where \( x \) and \( y \) are independent and uniform on \( \mathbb{F}_2^n \). Then there exists a linear function \( f : \mathbb{F}_2^n \to \mathbb{F}_2^n \) such that \( \text{Pr}[f(x)=\ell(x)] \geq \text{poly}(\epsilon) \).

• The PFR Conjecture is known to follow from the Polynomial Bogolyubov Conjecture \([GT09]\): Let \( A \subseteq \mathbb{F}_2^n \) have density at least \( \alpha \). Then \( A + A + A \) contains an affine subspace of codimension \( O(\log(1/\alpha)) \).

One can slightly weaken the Polynomial Bogolyubov Conjecture by replacing \( A + A + A \) with \( kA \) for an integer \( k > 3 \). It is known that any such weakening (for fixed finite \( k \)) is enough to imply the PFR Conjecture.

• Sanders \([San10b]\) has the best result in the direction of these conjectures, showing that if \( A \subseteq \mathbb{F}_2^n \) has density at least \( \alpha \) then \( A + A \) contains 99% of the points in a subspace of codimension \( O(\log(1/\alpha)) \), and hence \( 4A \) contains all of this subspace. This suffices to give the Freiman–Ruzsa Conjecture with \( 2^{O(\log^4 C)} \) in place of \( \text{poly}(C) \).

• Green and Tao \([GT09]\) have proved the Polynomial Freiman–Ruzsa Conjecture in the case that \( A \) is monotone.

**Mansour’s Conjecture**

**Statement:** Let \( f : \{-1,1\}^n \to \{-1,1\} \) be computable by a DNF of size \( s > 1 \) and let \( \epsilon \in (0,1/2] \). Then \( f \)'s Fourier spectrum is \( \epsilon \)-concentrated on a collection \( \mathcal{F} \) with \( |\mathcal{F}| \leq s^{O(\log(1/\epsilon))} \).

**Source:** \([Man94]\)

**Remarks:**

• Weaker version: replacing \( s^{O(\log(1/\epsilon))} \) by \( s^{O(1)} \).

• The weak version with bound \( s^{O(1/\epsilon)} \) is known to follow from the Fourier Entropy–Influence Conjecture.

• Proved for “almost all” polynomial-size DNF formulas (appropriately defined) by Klivans, Lee, and Wan \([KLW10]\).

• Mansour \([Man95]\) obtained the upper-bound \( (s/\epsilon)^{O(\log\log(s/\epsilon)\log(1/\epsilon))} \).

**Bernoulli Conjecture**

**Statement:** Let \( T \) be a finite collection of vectors in \( \mathbb{R}^n \). Define \( b(T) = E_{x \sim \{-1,1\}^n}[\max_{t \in T} \langle t, x \rangle] \), and define \( g(T) \) to be the same quantity except with \( x \sim \mathbb{R}^n \) Gaussian. Then there exists a finite collection of vectors \( T' \) such that \( g(T') \leq O(b(T)) \) and \( \forall t \in T \exists t' \in T' \|t - t'\|_1 \leq O(b(T)) \).

**Source:** \([Tal94]\)
Remarks:

- The quantity $g(T)$ is well-understood in terms of the geometry of $T$, thanks to Talagrand's majorizing measures theorem.
- Talagrand offers a $5000 prize for proving this, and a $1000 prize for disproving it.

### Fourier Entropy–Influence Conjecture

**Statement:** There is a universal constant $C$ such that for any $f : \{-1, 1\}^n \to \{-1, 1\}$ it holds that $H[\hat{f}^2] \leq C \cdot I[f]$, where $H[f^2] = \sum_S \hat{f}(S)^2 \log_2 \frac{1}{\hat{f}(S)^2}$ is the spectral entropy and $I[f]$ is the total influence.

**Source:** [FK96]

**Remarks:**

- Proved for “almost all” polynomial-size DNF formulas (appropriately defined) by Klivans, Lee, and Wan [KLM10].
- Proved for symmetric functions and functions computable by read-once decision trees by O’Donnell, Wright, and Zhou [OWZ11].
- An explicit example showing that $C \geq 60/13$ is necessary is known. (O’Donnell, unpublished.)
- Weaker version: the “Min-Entropy–Influence Conjecture”, which states that there exists $S$ such that $\hat{f}(S)^2 \geq 2^{-C \cdot I[f]}$. This conjecture is strictly stronger than the KKL Theorem, and is implied by the KKL Theorem in the case of monotone functions.

### Majority Is Least Stable Conjecture

**Statement:** Let $f : \{-1, 1\}^n \to \{-1, 1\}$ be a linear threshold function, $n$ odd. Then for all $\rho \in [0, 1]$, $\text{Stab}_\rho[f] \geq \text{Stab}_\rho[\text{Maj}_n]$.

**Source:** [BKS99]

**Remarks:**

- Slightly weaker version: If $f$ is a linear threshold function then $\text{NS}_\delta[f] \leq \frac{2}{n} \sqrt{\delta} + o(\sqrt{\delta})$.
- The best result towards the weaker version is Peres’s Theorem [Per04], which shows that every linear threshold function $f$ satisfies $\text{NS}_\delta[f] \leq \sqrt{\frac{2}{n}} \sqrt{\delta} + O(\delta^{3/2})$.
- By taking $\rho \to 0$, the conjecture has the following consequence, which is also open: Let $f : \{-1, 1\}^n \to \{-1, 1\}$ be a linear threshold function with $E[f] = 0$. Then $\sum_{i=1}^n \hat{f}(i)^2 \geq \frac{2}{n}$. The best known lower bound here is $\frac{1}{2}$, which follows from the Khinchine–Kahane inequality; see [GL94].
Optimality of Majorities for Non-Interactive Correlation Distillation

**Statement:** Fix \( r \in \mathbb{N}, n \) odd, and \( 0 < \epsilon < 1/2 \). For \( f : \{-1,1\}^n \to \{-1,1\} \), define \( P(f) = \Pr[f(y^{(1)}) = f(y^{(2)}) = \cdots = f(y^{(r)})] \), where \( x \sim \{-1,1\}^n \) is chosen uniformly and then each \( y^{(i)} \) is (independently) an \( \epsilon \)-noisy copy of \( x \). Is it true that \( P(f) \) is maximized among odd functions \( f \) by the Majority function \( \text{Maj}_k \) on some odd number of inputs \( k \)?

**Source:** [MO05] (originally from 2002)

**Remarks:**
- It is possible (e.g., for \( r = 10, n = 5, \epsilon = .26 \)) for neither the Dictator (\( \text{Maj}_1 \)) nor full Majority (\( \text{Maj}_n \)) to be maximizing.

Noise Sensitivity of Intersections of Halfspaces

**Statement:** Let \( f : \{-1,1\}^n \to \{-1,1\} \) be the intersection (AND) of \( k \) linear threshold functions. Then \( \text{NS}_\delta[f] \leq O \left( \sqrt{\log k} \right) \cdot \sqrt{\delta} \).

**Source:** [KOS02]

**Remarks:**
- The bound \( O(k) \cdot \sqrt{\delta} \) follows easily from Peres’s Theorem and is the best known.
- The “Gaussian special case” follows easily from the work of Nazarov [Naz03].
- An upper bound of the form \( \text{polylog}(k) \cdot \delta^{\Omega(1)} \) holds if the halfspaces are sufficiently “regular” [HKM10].

Non-Interactive Correlation Distillation with Erasures

**Statement:** Let \( f : \{-1,1\}^n \to \{-1,1\} \) be an unbiased function. Let \( z \sim \{-1,0,1\}^n \) be a “random restriction” in which each coordinate \( z_i \) is (independently) \( \pm 1 \) with probability \( p/2 \) each, and \( 0 \) with probability \( 1 - p \). Assuming \( p < 1/2 \) and \( n \) odd, is it true that \( E_z[|f(z)|] \) is maximized when \( f \) is the majority function? (Here we identify \( f \) with its multilinear expansion.)

**Source:** [Yan04]

**Remarks:**
- For \( p \geq 1/2 \), Yang conjectured that \( E_z[|f(z)|] \) is maximized when \( f \) is a dictator function; this was proved by O’Donnell and Wright [OW12].
- Mossel [Mos10] shows that if \( f \)’s influences are assumed at most \( \tau \) then \( E_z[|f(z)|] \leq E_z[|\text{Maj}_n(z)|] + o_{\tau}(1) \).

Triangle Removal in \( \mathbb{F}_2^n \)

**Statement:** Let \( A \subseteq \mathbb{F}_2^n \). Suppose that \( \epsilon 2^n \) elements must be removed from \( A \) in order to make it “triangle-free” (meaning there does not exist
Is it true that $\Pr_{x,y}[x,y,x+y \in A] \geq \text{poly}(\varepsilon)$, where $x$ and $y$ are independent and uniform on $\mathbb{F}_2^n$?

Source: [Gre05a]

Remarks:

- Green [Gre05a] showed the lower bound $1/(2\uparrow\uparrow \varepsilon - \Theta(1))$.
- Bhattacharyya and Xie [BX10] constructed an $A$ for which the probability is at most roughly $\varepsilon^{3.409}$.

### Subspaces in Sumsets

**Statement:** Fix a constant $\alpha > 0$. Let $A \subseteq \mathbb{F}_2^n$ have density at least $\alpha$. Is it true that $A + A$ contains a subspace of codimension $O(\sqrt{n})$?

Source: [Gre05a]

Remarks:

- The analogous problem for the group $\mathbb{Z}_N$ dates back to Bourgain [Bou90].
- By considering the Hamming ball $A = \{x : |x| \leq n/2 - \Theta(\sqrt{n})\}$, it is easy to show that codimension $O(\sqrt{n})$ cannot be improved. This example is essentially due to Ruzsa [Ruz93], see [Gre05a].
- The best bounds are due to Sanders [San10a], who shows that $A + A$ must contain a subspace of codimension $[n/(1 + \log_2(\frac{n}{1 - 2^\alpha}))]$. Thinking of $\alpha$ as small, this means a subspace of dimension roughly $\frac{\alpha}{\ln 2} \cdot n$. Thinking of $\alpha = 1/2 - \epsilon$ for $\epsilon$ small, this is codimension roughly $n/\log_2(1/\epsilon)$. In the same work Sanders also shows that if $\alpha \geq 1/2 - .001/\sqrt{n}$ then $A + A$ contains a subspace of codimension 1.
- As noted in the remarks on the Polynomial Freiman–Ruzsa/Bogolyubov Conjectures, it is also interesting to consider the relaxed problem where we only require that $A + A$ contains 99% of the points in a large subspace. Here it might be conjectured that the subspace can have codimension $O(\log(1/\alpha))$.

### Aaronson–Ambainis Conjecture

**Statement:** Let $f : \{-1,1\}^n \rightarrow [-1,1]$ have degree at most $k$. Then there exists $i \in [n]$ with $\text{Inf}_i[f] \geq (\text{Var}[f]/k)^{O(1)}$.

Source: [Aar08, AA11]

Remarks:

- True for $f : \{-1,1\}^n \rightarrow \{-1,1\}$; this follows from a result of O’Donnell, Schramm, Saks, and Servedio [OSSS05].
- The weaker lower bound $(\text{Var}[f]/2^k)^{O(1)}$ follows from a result of Dinur, Kindler, Friedgut, and O’Donnell [DFKO07].
Bhattacharyya–Grigorescu–Shapira Conjecture

Statement: Let $M \in \mathbb{F}_2^{m \times k}$ and $\sigma \in \{0, 1\}^k$. Say that $f : \mathbb{F}_2^n \to \{0, 1\}$ is $(M, \sigma)$-free if there does not exist $X = (x^{(1)}, \ldots, x^{(k)})$ (where each $x^{(j)} \in \mathbb{F}_2^n$ is a row vector) such that $MX = 0$ and $f(x^{(j)}) = \sigma_j$ for all $j \in [k]$. Now fix a (possibly infinite) collection $(M^1, \sigma^1), (M^2, \sigma^2), \ldots$ and consider the property $\mathcal{P}_n$ of functions $f : \mathbb{F}_2^n \to \{0, 1\}$ that $f$ is $(M^i, \sigma^i)$-free for all $i$. Then there is a one-sided error, constant-query property-testing algorithm for $\mathcal{P}_n$.

Source: [BGS10]

Remarks:

- The conjecture is motivated by a work of Kaufman and Sudan [KS08] which proposes as an open research problem the characterization of testability for linear-invariant properties of functions $f : \mathbb{F}_2^n \to \{0, 1\}$. The properties defined in the conjecture are linear-invariant.
- Every property family $(\mathcal{P}_n)$ defined by $((M^1, \sigma^1), (M^2, \sigma^2), \ldots)$-freeness is subspace-hereditary; i.e., closed under restriction to subspaces. The converse also “essentially” holds. [BGS10].
- For $M$ of rank one, Green [Gre05a] showed that $(M, 1^k)$-freeness is testable. He conjectured this result extends to arbitrary $M$; this was confirmed by Král’, Serra, and Vena [KSV08] and also Shapira [Sha09]. Austin [Sha09] subsequently conjectured that $(M, \sigma)$-freeness is testable for arbitrary $\sigma$; even this subcase is still open.
- The conjecture is known to hold when all $M^i$ have rank one [BGS10]. Also, Bhattacharyya, Fischer, and Lovett [BFL12] have proved the conjecture in the setting of $\mathbb{F}_p$ for affine constraints $((M^1, \sigma^1), (M^2, \sigma^2), \ldots)$ of “Cauchy–Schwarz complexity” less than $p$.

Symmetric Gaussian Problem

Statement: Fix $0 \leq \rho, \mu, \nu \leq 1$. Suppose $A, B \subseteq \mathbb{R}^n$ have Gaussian measure $\mu$, $\nu$ respectively. Further, suppose $A$ is centrally symmetric: $A = -A$. What is the minimal possible value of $\text{Pr}[x \in A, y \in B]$, when $(x, y)$ are $\rho$-correlated $n$-dimensional Gaussians?

Source: [CR10]

Remarks:

- It is equivalent to require both $A = -A$ and $B = -B$.
- Without the symmetry requirement, the minimum occurs when $A$ and $B$ are opposing halfspaces; this follows from the work of Borell [Bor85].
- A reasonable conjecture is that the minimum occurs when $A$ is a centered ball and $B$ is the complement of a centered ball.
Standard Simplex Conjecture
Statement: Fix $0 \leq \rho \leq 1$. Then among all partitions of $\mathbb{R}^n$ into $3 \leq q \leq n + 1$ parts of equal Gaussian measure, the maximal noise stability at $\rho$ occurs for a “standard simplex partition”. By this it is meant a partition $A_1, \ldots, A_q$ satisfying $A_i \supseteq \{x \in \mathbb{R}^n : \langle a_i, x \rangle > \langle a_j, x \rangle \forall j \neq i \}$, where $a_1, \ldots, a_q \in \mathbb{R}^n$ are unit vectors satisfying $\langle a_i, a_j \rangle = -\frac{1}{q-1}$ for all $i \neq j$. Further, for $-1 \leq \rho \leq 0$ the standard simplex partition minimizes noise stability at $\rho$.
Source: [IM09]
Remarks:
- Implies the Plurality Is Stablest Conjecture of Khot, Kindler, Mossel, and O’Donnell [KKMO04]; in turn, the Plurality Is Stablest Conjecture implies it for $\rho \geq -\frac{1}{q-1}$.

Linear Coefficients versus Total Degree
Statement: Let $f : \{-1, 1\}^n \to \{-1, 1\}$. Then $\sum_{i=1}^n \hat{f}(i) \leq \sqrt{\deg(f)}$.
Source: Parikshit Gopalan and Rocco Servedio, ca. 2009
Remarks:
- More ambitiously, one could propose the upper bound $k \cdot \left(\frac{k-1}{2^k}\right)2^{1-k}$, where $k = \deg(f)$. This is achieved by the Majority function on $k$ bits.
- Apparently, no bound better than the trivial $\sum_{i=1}^n \hat{f}(i) \leq \|f\| \leq \deg(f)$ is known.

$k$-wise Independence for PTFs
Statement: Fix $d \in \mathbb{N}$ and $\epsilon \in (0, 1)$. Determine the least $k = k(d, \epsilon)$ such that the following holds: If $p : \mathbb{R}^n \to \mathbb{R}$ is any degree-$d$ multivariate polynomial, and $X$ is any $\mathbb{R}^n$-valued random variable with the property that each $X_i$ has the standard Gaussian distribution and each collection $X_i, \ldots, X_{ik}$ is independent, then $|\Pr[p(X) \geq 0] - \Pr[p(Z) \geq 0]| \leq \epsilon$, where $Z$ has the standard $n$-dimensional Gaussian distribution.
Source: [DGJ*09]
Remarks:
- For $d = 1$, Diakonikolas, Gopalan, Jaiswal, Servedio, and Viola [DGJ*09] showed that $k = O(1/\epsilon^2)$ suffices. For $d = 2$, Diakonikolas, Kane, and Nelson [DKN10] showed that $k = O(1/\epsilon^4)$ suffices. For general $d$, Kane [Kan11] showed that $O_d(1) \cdot \epsilon^{2^d}$ suffices and that $\Omega(d^2/\epsilon^2)$ is necessary.

$\epsilon$-biased Sets for DNFs
Statement: Is it true for each constant $\delta > 0$ that $s^{\Omega(1)}$-biased densities
δ-fool size-s DNFs? I.e., that if $f : \{0,1\}^n \rightarrow \{-1,1\}$ is computable by a size-s DNF and $\varphi$ is an $s^{-O(1)}$-biased density on $\{0,1\}$, then $|E_{x \sim \{0,1\}^n}[f(x)] - E_{y \sim \varphi}[f(y)]| \leq \delta$.

**Source:** [DETT10], though the problem of pseudorandom generators for bounded-depth circuits dates back to [AW85]

**Remarks:**
- De, Etessami, Trevisan, and Tulsiani [DETT10] show the result for $\exp(-O(\log^2(s) \log \log s))$-biased densities. If one assumes Mansour's Conjecture, their result improves to $\exp(-O(\log^2 s))$. More precisely, they show that $\exp(-O(\log^2(s/\delta) \log \log(s/\delta)))$-biased densities $\delta$-fool size-s DNF. They also give an example showing that $s^{-O(\log(1/\delta))}$-biased densities are necessary. Finally, they show that $s^{-O(\log(1/\delta))}$-biased densities suffice for read-once DNFs.

**PTF Sparsity for Inner Product Mod 2**

**Statement:** Is it true that any PTF representation of the inner product mod 2 function on $2^n$ bits, $\text{IP}_{2^n} : \mathbb{F}_2^{2n} \rightarrow \{-1,1\}$, requires at least $3^n$ monomials?

**Source:** Srikanth Srinivasan, 2010

**Remarks:**
- Rocco Servedio independently asked if the following much stronger statement is true: Suppose $f, g : \{-1,1\}^n \rightarrow \{-1,1\}$ require PTFs of sparsity at least $s, t$, respectively; then $f \circ g : \{-1,1\}^{2n} \rightarrow \{-1,1\}$ (the function $(x, y) \mapsto f(x)g(y)$) requires PTFs of sparsity at least $st$.

**Servio–Tan–Verbin Conjecture**

**Statement:** Fix any $\epsilon > 0$. Then every monotone $f : \{-1,1\}^n \rightarrow \{-1,1\}$ is $\epsilon$-close to a $\text{poly}(\text{deg}(f))$-junta.

**Source:** Elad Verbin (2010) and independently Rocco Servedio and Li-Yang Tan (2010)

**Remarks:**
- One can equivalently replace degree by decision-tree depth or maximum sensitivity.
- RESOLVED (in the negative) by Daniel Kane, 2012.

**Average versus Max Sensitivity for Monotone Functions**

**Statement:** Let $f : \{-1,1\}^n \rightarrow \{-1,1\}$ be monotone. Then $\text{I}[f] < o(\text{sens}[f])$.

**Source:** Rocco Servedio, Li-Yang Tan, 2010

**Remarks:**
• The tightest example known has $I[f] \approx \text{sens}[f]^{61}$; this appears in a work of O’Donnell and Servedio [OS08].

**Approximate Degree for Approximate Majority**

**Statement:** What is the least possible degree of a function $f : \{-1, 1\}^n \to [-1, -2/3] \cup [2/3, 1]$ which has $f(x) \in [2/3, 1]$ whenever $\sum_{i=1}^n x_i \geq n/2$ and has $f(x) \in [-1, -2/3]$ whenever $\sum_{i=1}^n x_i \leq -n/2$?

**Source:** Srikanth Srinivasan, 2010

**Remarks:**

• Note that $f(x)$ is still required to be in $[-1, -2/3] \cup [2/3, 1]$ when $-n/2 < \sum_{i=1}^n x_i < n/2$.

**Uncertainty Principle for Quadratic Fourier Analysis**

**Statement:** Suppose $q_1, \ldots, q_m : \mathbb{F}_2^n \to \mathbb{F}_2$ are polynomials of degree at most 2 and suppose the indicator function of $(1, \ldots, 1) \in \mathbb{F}_2^n$, namely $\text{AND} : \mathbb{F}_2^n \to \{-1, 1\}$, is expressible as $\text{AND}(x) = \sum_{i=1}^m c_i(-1)^{q_i(x)}$ for some real numbers $c_i$. What is a lower bound for $m$?

**Source:** Hamed Hatami, 2011

**Remarks:**

• Hatami can show that $m \geq n$ is necessary but conjectures $m \geq 2^{\Omega(n)}$ is necessary. Note that if the $q_i$’s are of degree at most 1 then $m = 2^n$ is necessary and sufficient.

• The **Constant-Degree Hypothesis** is a similar conjecture made by Barrington, Straubing, and Thérien [BST90] in 1990 in the context of finite fields.
## Bibliography

[Aa11] Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. In *Proceedings of the 2nd Annual Symposium on Innovations in Computer Science*, 2011.

[Aar08] Scott Aaronson. How to solve longstanding open problems in quantum computing using only Fourier Analysis. Invited lecture at Banff International Research Station, 2008. [http://www.scottaaronson.com/talks/openqc.ppt](http://www.scottaaronson.com/talks/openqc.ppt).

[AW85] Miklós Ajtai and Avi Wigderson. Deterministic simulation of probabilistic constant depth circuits. In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science*, pages 11–19, 1985.

[BBB+10] Keith Ball, Franck Barthe, Witold Bednorz, Krzysztof Oleszkiewicz, and Paweł Wolff. $L^1$-smoothing for the Ornstein–Uhlenbeck semigroup. [http://www2.warwick.ac.uk/fac/sci/maths/people/staff/keith_ball/2010-09-21-gaussian.pdf](http://www2.warwick.ac.uk/fac/sci/maths/people/staff/keith_ball/2010-09-21-gaussian.pdf), 2010.

[BFL12] Arnab Bhattacharyya, Eldar Fischer, and Shachar Lovett. Testing low complexity affine-invariant properties. Technical Report 1201.0330, arXiv, 2012.

[BGS10] Arnab Bhattacharyya, Elena Grigorescu, and Asaf Shapira. A unified framework for testing linear-invariant properties. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science*, pages 478–487, 2010.
[BKS99] Itai Benjamini, Gil Kalai, and Oded Schramm. Noise sensitivity of Boolean functions and applications to percolation. *Publications Mathématiques de l'IHÉS*, 90(1):5–43, 1999.

[BNS92] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *Journal of Computer and System Sciences*, 45(2):204–232, 1992.

[Bor85] Christer Borell. Geometric bounds on the Ornstein-Uhlenbeck velocity process. *Probability Theory and Related Fields*, 70(1):1–13, 1985.

[Bou90] Jean Bourgain. *A tribute to Paul Erdős*, chapter On arithmetic progressions in sums of sets of integers, pages 105–109. Cambridge University Press, 1990.

[Bou05] Jean Bourgain. Estimation of certain exponential sums arising in complexity theory. *Comptes Rendus Mathematique*, 340(9):627–631, 2005.

[BST90] David Mix Barrington, Howard Straubing, and Denis Thérien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, 1990.

[BX10] Arnab Bhattacharyya and Ning Xie. Lower bounds for testing triangle-freeness in Boolean functions. In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 87–98, 2010.

[CFG88] Fan Chung, Zoltán Füredi, Ronald Graham, and Paul Seymour. On induced subgraphs of the cube. *J. Comb. Theory A*, 49:180–187, 1988.

[CR10] Amit Chakrabarti and Oded Regev. An optimal lower bound on the communication complexity of Gap-Hamming-Distance. In *Electronic Colloquium on Computational Complexity TR10-140*, 2010.

[DETT10] Anindya De, Omid Etesami, Luca Trevisan, and Madhur Tulsi. Improved pseudorandom generators for depth 2 circuits.
In *Proceedings of the 14th Annual International Workshop on Randomized Techniques in Computation*, pages 504–517, 2010.

[DFKO07] Irit Dinur, Ehud Friedgut, Guy Kindler, and Ryan O’Donnell. On the Fourier tails of bounded functions over the discrete cube. *Israel Journal of Mathematics*, 160(1):389–412, 2007.

[DGJ*09] Ilias Diakoniokolas, Parikshit Gopalan, Ragesh Jaiswal, Rocco Servedio, and Emanuele Viola. Bounded independence fools halfspaces. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 171–180, 2009.

[DHK*10] Ilias Diakonikolas, Prahladh Harsha, Adam Klivans, Raghu Meka, Prasad Raghavendra, Rocco Servedio, and Li-Yang Tan. Bounding the average sensitivity and noise sensitivity of polynomial threshold functions. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, pages 533–542, 2010.

[DKN10] Ilias Diakonikolas, Daniel Kane, and Jelani Nelson. Bounded independence fools degree-2 threshold functions. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science*, pages 11–20, 2010.

[FK96] Ehud Friedgut and Gil Kalai. Every monotone graph property has a sharp threshold. *Proceedings of the American Mathematical Society*, 124(10):2993–3002, 1996.

[GL92] Craig Gotsman and Nathan Linial. The equivalence of two problems on the cube. *Journal of Combinatorial Theory, Series A*, 61(1):142–146, 1992.

[GL94] Craig Gotsman and Nathan Linial. Spectral properties of threshold functions. *Combinatorica*, 14(1):35–50, 1994.

[Gre05a] Ben Green. A Szemerédi-type regularity lemma in abelian groups, with applications. *Geometric And Functional Analysis*, 15(2):340–376, 2005.

[Gre05b] Ben Green. Finite field models in additive combinatorics. In *London Mathematical Society Lecture Notes*, volume 327, pages 1–27, Cambridge University Press, 2005.
[GRS05] Frederic Green, Amitabha Roy, and Howard Straubing. Bounds on an exponential sum arising in boolean circuit complexity. Comptes Rendus Mathematique, 341(5):279–282, 2005.

[GT09] Ben Green and Terence Tao. Freiman’s theorem in finite fields via extremal set theory. Combinatorics, Probability and Computing, 18(3):335–355, 2009.

[Guy89] Richard Guy. Any answers anent these analytical enigmas? American Mathematical Monthly, 93(4):279–281, 1989.

[HK92] Ron Holzman and Daniel Kleitman. On the product of sign vectors and unit vectors. Combinatorica, 12(3):303–316, 1992.

[HKM10] Prahladh Harsha, Adam Klivans, and Raghu Meka. An invariance principle for polytopes. In Proceedings of the 42nd Annual ACM Symposium on Theory of Computing, pages 543–552, 2010.

[IM09] Marcus Isaksson and Elchanan Mossel. Maximally stable Gaussian partitions with discrete applications. Technical Report 0903.3362, arXiv, 2009.

[Kan09] Daniel Kane. The Gaussian surface area and noise sensitivity of degree-\(d\) polynomials. Technical Report 0912.2709, arXiv, 2009.

[Kan11] Daniel Kane. A small PRG for polynomial threshold functions of Gaussians. In Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science, pages 257–266, 2011.

[KKMO04] Subhash Khot, Guy Kindler, Elchanan Mossel, and Ryan O’Donnell. Optimal inapproximability results for MAX-CUT and other 2-variable CSPs? In Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, 2004.

[KLW10] Adam Klivans, Homin Lee, and Andrew Wan. Mansour’s Conjecture is true for random DNF formulas. In Proceedings of the 23rd Annual Conference on Learning Theory, pages 368–380, 2010.

[KOS02] Adam Klivans, Ryan O’Donnell, and Rocco Servedio. Learning intersections and thresholds of halfspaces. In Proceedings of the
43rd Annual IEEE Symposium on Foundations of Computer Science, pages 177–186, 2002.

[KS08] Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In Proceedings of the 40th Annual ACM Symposium on Theory of Computing, pages 403–412, 2008.

[KSV08] Daniel Král’, Oriol Serra, and Lluís Vena. A removal lemma for systems of linear equations over finite fields. Technical Report 0809.1846, arXiv, 2008.

[Man94] Yishay Mansour. Learning Boolean functions via the Fourier Transform. In Vwani Roychowdhury, Kai-Yeung Siu, and Alon Orlitsky, editors, Theoretical Advances in Neural Computation and Learning, chapter 11, pages 391–424. Kluwer Academic Publishers, 1994.

[Man95] Yishay Mansour. An $O(n \log \log n)$ learning algorithm for DNF under the uniform distribution. Journal of Computer and System Sciences, 50(3):543–550, 1995.

[MO05] Elchanan Mossel and Ryan O’Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. Random Structures & Algorithms, 26(4):418–436, 2005.

[Mos10] Elchanan Mossel. Gaussian bounds for noise correlation of functions. Geometric and Functional Analysis, 19(6):1713–1756, 2010.

[Naz03] Fedor Nazarov. On the maximal perimeter of a convex set in $\mathbb{R}^n$ with respect to a Gaussian measure. In Geometric Aspects of Functional Analysis, volume 1807, pages 169–187. Israel Seminar, 2003.

[NS94] Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. Computational Complexity, 4(4):301–313, 1994.

[OS08] Ryan O’Donnell and Rocco Servedio. Learning monotone decision trees in polynomial time. SIAM Journal on Computing, 37(3):827–844, 2008.
[OSSS05] Ryan O'Donnell, Michael Saks, Oded Schramm, and Rocco Servedio. Every decision tree has an influential variable. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 31–39, 2005.

[OW12] Ryan O'Donnell and John Wright. A new point of NP-hardness for Unique-Games. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, 2012.

[OWZ11] Ryan O'Donnell, Yi Wu, and Yuan Zhou. Optimal lower bounds for locality sensitive hashing (except when q is tiny). In *Proceedings of the 2nd Annual Symposium on Innovations in Computer Science*, 2011.

[Per04] Yuval Peres. Noise stability of weighted majority. Technical Report 0412377, arXiv, 2004.

[Raz87] Alexander Razborov. Lower bounds on the dimension of schemes of bounded depth in a complete basis containing the logical addition function. *Matematicheskie Zametki*, 41(4):598–607, 1987.

[Ruz93] Imre Ruzsa. An analog of Freiman’s theorem in groups. Technical Report 77, DIMACS, 1993.

[San10a] Tom Sanders. Green’s sumset problem at density one half. Technical Report 1003.5649, arXiv, 2010.

[San10b] Tom Sanders. On the Bogolyubov–Ruzsa lemma. Technical Report 1011.0107, arXiv, 2010.

[Sha09] Asaf Shapira. Green’s conjecture and testing linear-invariant properties. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 159–166, 2009.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 77–82, 1987.

[Sze89] Mario Szegedy. *Algebraic methods in lower bounds for computational models with limited communication*. PhD thesis, University of Chicago, 1989.
[Tal89] Michel Talagrand. A conjecture on convolution operators, and a non-Dunford–Pettis operator on $L^1$. *Israel Journal of Mathematics*, 68(1):82–88, 1989.

[Tal94] Michel Talagrand. Constructions of majorizing measures, Bernoulli processes and cotype. *Geometric and Functional analysis*, 4(6):660–717, 1994.

[VW08] Emanuele Viola and Avi Wigderson. Norms, XOR lemmas, and lower bounds for $gf(2)$ polynomials and multiparty protocols. *Theory of Computing*, 4:137–168, 2008.

[Yan04] Ke Yang. On the (im)possibility of non-interactive correlation distillation. In *Proceedings of the 6th Annual Latin American Informatics Symposium*, pages 222–231, 2004.