# Lower bounds for $k$-DNF Resolution on random 3-CNFs

Sergey Nurk

Mathematics and Mechanics Faculty
Saint-Petersburg State University

JASS, 2009

# Outline

# Resolution

## Resolution Rule

A,B - clauses
$$\frac{A \vee x \quad \neg x \vee B}{A \vee B}$$

## Definition

- The *width* $\omega(C)$ of a clause $C$ is the number of literals in $C$.
- The *width* $\omega(\tau)$ of a set of clauses $\tau$ (in particular the width of a resolution proof) is the maximal width of the clauses appearing in this set.
- The *size* of a resolution proof is the number of different clauses in it.

# Resolution

## Definition

Consider an unsatisfiable set of clauses $\tau$. Denote by $S_R(\tau)$ the size of minimal refutation of $\tau$. Denote by $\omega_R(\tau)$ the minimal refutation width over all possible proofs of $\tau$.

## Weakening

We will extend *Resolution* with *weakening* inferences:

$A, B$-clauses. If $A \subseteq B$, then $\dfrac{A}{B}$.

# What is Res($k$)?

*$k$-DNF Resolution* (*Res*($k$)) is a generalization of *Resolution* that operates with $k$-DNFs instead of clauses.

## Res($k$) Inference Rules

A, B are $k$-DNFs, $1 \leq j \leq k$ and $l, l_1, \ldots, l_j$ are literals

- Weakening: $\dfrac{A}{A \vee l}$
- Cut: $\dfrac{A \vee \bigwedge_{i=1}^{j} l_i \quad B \vee \bigvee_{i=1}^{j} \neg l_i}{A \vee B}$
- AND-introduction: $\dfrac{A \vee l_1 \ldots A \vee l_j}{A \vee \bigwedge_{i=1}^{j} l_i}$
- AND-elimination: $\dfrac{A \vee \bigwedge_{i=1}^{j} l_i}{A \vee l_i}$

**Remark:** *Resolution* $=$ *Res*$(1)$.

# Strong Soundness

**Important property:** *Res*($k$) *is strongly sound.*
If *k-DNF* $F$ is inferred from *k-DNFs* $F_1, \ldots, F_j$, and $t_1, \ldots, t_j$ are mutually consistent terms of $F_1, \ldots, F_j$ respectively, then there is a term $t$ of $F$ implied by $\bigwedge_{i=1}^{j} t_i$.

# Related Definitions

**Definition**

*Res*($k$) *refutation* of unsatisfiable CNF $\tau$ is the inference of the empty clause from the clauses in $\tau$ using inference rules.

**Definition**

The *size* of *Res*($k$) refutation is the number of lines it contains.

**Definition**

$S_{R(k)}(\tau)$ denotes the minimal size of a *Res*($k$) refutation of CNF $\tau$.

# *Res*($k$) vs *Res*($k+1$)

Fact:

*Res*($k+1$) is exponentially more powerful than *Res*($k$).

# Decision Tree

## Definition

*Decision tree:*

- Rooted binary tree.
- Every internal node labeled with variable.
- Edges leaving node correspond to whether the variable is set to 0 or 1.
- Leaves are labeled with either 0 or 1.

**Remark:** Every path from the root to a leaf may be viewed as a partial assignment.

# Related Definitions

$v \in \{0, 1\}$, decision tree $T$, *DNF* $F$

**Definition**

$Br_v(T)$ denotes the set of paths that lead from the root to a leaf labeled $v$.

**Definition**

*$T$ strongly represents $F$* if for every $\pi \in Br_0(T)$, for all $t \in F, t|_\pi = 0$ and for every $\pi \in Br_1(T)$ there exists $t \in F, t|_\pi = 1$.

**Definition**

*Representation height* of $F$, $h(F)$, is the minimal height of a decision tree strongly representing $F$.

# Switching Lemma

## Definition

*DNF* $F$, set of variables $S$.
If every term of $F$ contains a variable from $S$, then $S$ is a cover of $F$. The *covering number* of $F$, $c(F)$, is the minimal cardinality of a cover of $F$.

## Switching Lemma

Let $k \geq 1$, let $s_0, \ldots, s_{k-1}$ and $p_1, \ldots, p_k$ be sequences of positive numbers, and let $D$ be a distribution on partial assignments so that for every $i \leq k$ and every $i$-*DNF* $G$, if $c(G) > s_{i-1}$, then $Pr_{\rho \in D}[G|_\rho \neq 1] \leq p_i$. Then for every $k$-*DNF* $F$:

$$Pr_{\rho \in D}\left[h(F|_\rho) > \sum_{i=0}^{k-1} s_i\right] \leq \sum_{i=1}^{k} 2^{(\sum_{j=i}^{k-1} s_j)} p_i$$

# Proof of Switching Lemma

## Proof.

- Induction on $k$.
- $k = 1$: If $c(F) \leq s_0$ then at most $s_0$ variables appear in $F$. If $c(F) > s_0$ then $Pr(h(F|_\rho) \neq 0) \leq Pr_{\rho \in D}[F|_\rho \neq 1] \leq p_1$
- $k \to k+1$ : $(k+1)$-$DNF$ $F$.
- If $c(F) > s_k$ then $Pr(h(F|_\rho) \neq 0) \leq Pr_{\rho \in D}[F|_\rho \neq 1] \leq p_{k+1}$
- Consider $c(F) \leq s_k$. $S$ is a cover of size at most $s_k$. $\pi$–assignment to the variables in $S$. $F|_\pi$ is a k-DNF. $Pr_{\rho \in D}\left[\exists \pi \in \{0,1\}^S : h((F|_\rho)|_\pi) > \sum_{i=0}^{k-1} s_i\right] \leq$ $2^{s_k}(\sum_{i=1}^{k} 2^{(\sum_{j=i}^{k-1} s_j)} p_i) < \sum_{i=1}^{k+1} 2^{(\sum_{j=i}^{k} s_j)} p_i$
- If $\forall \pi \in \{0,1\}^S$ $h((F|_\rho)|_\pi) \leq \sum_{i=0}^{k-1} s_i$ then we may construct a decision tree of height at most $\sum_{j=i}^{k} s_j$ strongly representing $F|_\rho$.

$\square$

# One More Switching Lemma

## Corollary

$k, s, d$ are positive integers, $\gamma, \delta \in (0,1]$. $D$ is a distribution on partial assignments s.t. $\forall$ *k-DNF G* $Pr_{\rho \in D}[G|_\rho \neq 1] \leq d2^{-\delta(c(G))^\gamma}$. For every *k-DNF F*:

$$Pr_{\rho \in D}[h(F|_\rho) > 2s] \leq dk2^{-\delta' s^{\gamma'}}$$

where $\delta' = 2(\delta/4)^k$ and $\gamma' = \gamma^k$.

# Proof of the Corollary

## Proof.

- $s_i = (\delta/4)^i s^{\gamma^i}$, $p_i = d2^{-4s_i}$.
- $s_{i-1}/4 \geq (\delta/4)s_{i-1} = (\delta/4)^i s^{\gamma^{i-1}} \geq s_i$. So $\sum_{j=i}^{k} s_j \leq \sum_{j\geq i} s_i/4^{j-i} \leq 2s_i$
- For any $i$-DNF $G$ with $c(G) \geq s_{i-1}$ $\quad Pr_{\rho\in D}[G|_\rho \neq 1] \leq d2^{-\delta(c(G))^\gamma} \leq d2^{-\delta s_{i-1}^{\gamma}} = 2^{-\delta(\delta/4)^{i-1}(s^{\gamma^{i-1}})^\gamma} = d2^{-4s_i}$
- After applying previous theorem we have that:
  For every $k$-DNF $F$ $\quad Pr_{\rho\in D}[h(F|_\rho) > 2s] \leq Pr_{\rho\in D}\left[h(F|_\rho) > \sum_{i=0}^{k-1} s_i\right] \leq \sum_{i=1}^{k} 2^{(\sum_{j=i}^{k-1} s_j)} p_i \leq \sum_{i=1}^{k} 2^{2s_i}(d2^{-4s_i}) \leq dk2^{-2s_k} = dk2^{-\delta' s^{\gamma'}}$

$\square$

# $Res(k) \longrightarrow Resolution$

## Theorem

*Let $\tau$ be a set of clauses s.t. $\omega(\tau) \leq h$. If $\tau$ has a $Res(k)$ refutation s.t. for each line $F$ of the refutation $h(F) \leq h$, then $\omega_R(\tau) \leq kh$.*

## Proof:

- $T_C$ is a decision tree for $C \in \tau$. For any line $F$ $T_F$ is a min height tree for $F$. For any partial assignment $\pi$ $C_\pi$ is a clause that contains negations of every literal in $\pi$.
- For $\pi \in Br_0(T_\emptyset)$, $C_\pi = \emptyset$ and for each $C \in \tau$ for the unique $\pi \in Br_0(T_C)$, $C_\pi = C$. We construct narrow resolution refutation by deriving $C_\pi$ for each line $F$ and each $\pi \in Br_0(T_F)$.

# Proof part 2

## Proof.

- Consider $F$ inferred from previously derived $F_1, \ldots, F_j$, $j \leq k$. We construct a decision tree $T$ of height $\leq kh$ that represents $\bigwedge_{i=1}^{j} F_i$.
- The set $\{C_\sigma | \sigma \in Br_0(T)\}$ can be derived using the weakening rule.
- For every $\sigma \in Br_1(T)$ there exists $t \in F$ satisfied by $\sigma$.
- Let $\pi \in Br_0(T_F)$ be given. For all $\sigma \in Br(T)$ consistent with $\pi$ $\sigma \in Br_0(T)$.
- For each node $\nu$ in $T$ $\sigma_\nu$ is the path from the root to $\nu$. From the leaves to the root , we derive $C_{\sigma_\nu} \vee C_\pi$ for each $\nu$ so that $\sigma_\nu$ is consistent with $\pi$. When we reach the root we will have derived $C_\pi$.

$\square$

# Random 3-CNF's and Linear Systems

## Definition

Denote by $\phi_{n,\Delta n}$ the random $3 - CNF$ with $\Delta n$ clauses and $n$ variables, in which every clause is chosen independently from the set of all $2^3 C_n^3$ clauses.

## Definition

For each $\phi_{n,\Delta}$ we consider a $\Delta n \times n$ matrix $A_{n,\Delta n}$ and a vector $b \in \{0, 1\}^{\Delta n}$ s.t.:

- $A_{n,\Delta n}[i, j] = 1$ iff the $i$-th clause of $\phi_{n,\Delta}$ contains the variable $x_j$.
- $b[i] =$ (number of positive variables in the $i$-th clause) $mod$ 2.

**Remark:** Each clause of $\phi_{n,\Delta n}$ is a semantical corollary of some linear equation of the system $A_{n,\Delta n}x = b$

# Expanders

$A \in \{0,1\}^{m \times n}$, $I \subseteq [m]$, $A_i$-$i$th row of A.

## Definition

*Boundary of I, $\partial I$, is a set of all $j \in [n]$ s.t. $\exists!\, i \in I : j \in A_i$*

## Definition

$A$ is an $(r, c)$-*boundary expander* if

$$\forall I \subseteq [m]\ \ (|I| \leq r \Rightarrow |\partial I| \geq c|I|)$$

## Fact:

$\forall \Delta > 0, c < 1\ \exists \delta$ s.t. with probability $1 - o(1)$ $A_{n,\Delta n}$ is $(\delta n, c)$-boundary expander.

# $Cl$

$A \in \{0,1\}^{m \times n}$, $J \subseteq [n]$, $\quad I, I_1 \subseteq [m]$

$$I \vdash_J I_1 \iff |I_1| \leq r/2 \, \wedge \, \partial(I_1) \subseteq \left[\bigcup_{i \in I} A_i \cup J\right]$$

## Definition

*Closure* $J$, $Cl(J)$, is a set of all rows which can be inferred from the empty set.

## Lemma

*If* $|J| \leq cr/2$ *then* $|Cl(J)| \leq c^{-1}|J|$

# Proof

**Proof.**

- $\{I_k\}$ s.t. $I_1 \cup \cdots \cup I_{\nu-1} \vdash_J I_\nu$.
- Consider the smallest $k$ s.t. $|\bigcup_{\nu=1}^{k} I_\nu| > c^{-1}|J|$
- Since $|J| \leq cr/2 \quad |\bigcup_{\nu=1}^{k} I_\nu| \leq r$ and since we are dealing with expander $|\partial(\bigcup_{\nu=1}^{k} I_\nu)| > c(c^{-1}|J|) = |J|$
- But $\partial(\bigcup_{\nu=1}^{k} I_\nu) \subseteq J$

$\square$

# $Cl^e$

$A \in \{0,1\}^{m\times n}$, $J \subseteq [n]$, $\quad I, I_1 \subseteq [m]$

$$I \vdash_J^e I_1 \iff |I_1| \leq r/2 \,\wedge\, \left|\partial(I_1) \setminus \left[\bigcup_{i\in I} A_i \cup J\right]\right| < (c/2)|I_1|$$

## Algorithm $Cl^e(J)$

$I := \emptyset$ $R := [m]$
**while** (there exists $I_1 \in R$ s.t. $I \vdash_J^e I_1$)
$I := I \cup I_1$
$R := R \setminus I_1$
**end**
output $I$;

## Lemma

*If* $|J| < cr/4$ *then* $|Cl^e(J)| < 2c^{-1}|J|$

# Proof

## Proof.

- Consider the sequence $I_1 \dots I_l$ appearing in the cleaning procedure. These sets are pairwise disjoint.
- $C_t := \bigcup_{k=1}^{t} I_k$. By $T$ denote the first $t : |C_t| > 2c^{-1}|J|$
- Since $|J| < cr/4 \quad |C_T| \leq r$
- Due to expansion $|\partial C_T| > c|C_T|$, so $|\partial C_T \setminus J| > c|C_T| - |J| \geq c|C_T|/2$
- But $|\partial C_T \setminus J| \leq c/2 \sum_{k=1}^{T} |I_k| = c/2|C_T|$

$\square$

# A little more about $Cl^e$

$A \in \{0,1\}^{m\times n}$, $J \subseteq [n]$
$I' = Cl^e(J),\ J' = \bigcup_{i\in I'} A_i$.

## Lemma

*Obtain $\hat{A}$ by removing the rows corresponding to $I'$ and columns to $J'$. $\hat{A}$ is either empty or $(r/2, c/2)$-boundary expander.*

## Proof.

- Consider $I \in \hat{A} : |I| \leq r/2$. $\partial_A I \subseteq \partial_{\hat{A}} I \cup J \cup J'$
- If $|\partial_{\hat{A}} I| < (c/2)|I|$ then $|\partial_A I \setminus (J' \cup J)| < (c/2)|I|$ and $I' \vdash_J^e I$.

$\square$

# Local Consistence

For a term $t$ $Cl(t) := Cl(Vars(t))$ and $Cl^e(t) := Cl^e(Vars(t))$
$A \in \{0,1\}^{m\times n},\ b \in \{0,1\}^m$

## Definition

Term $t$ is *locally consistent* w.r.t. $Ax = b$ if the formula $t \wedge [A_I x = b_I]$ is satisfiable, where $I = Cl(t)$.

## Lemma

*If $t$ is locally consistent then $\forall I \subseteq [m] : |I| < r/2$ the formula $t \wedge [A_I x = b_I]$ is satisfiable.*

## Proof.

If not then $\exists t' \in t, I' \in I$ s.t. $\sum_{i\in I'}(A_i x - b_i) + \sum_{x_j^\epsilon \in t'}(x_j - \epsilon) \equiv 1$
Then $\partial(I') \in Vars(t')$, hence $I' \in Cl(t)$ and $t$ is inconsistent. $\square$

$A \in \{0, 1\}^{m \times n}$

## Definition

$G(A)$ is the bipartite graph between m row vertices and n column vertices with incidence matrix $A$. $d_A(V_1, V_2)$ denotes the shortest path between sets $V_1, V_2$ in $G(A)$

## Lemma

*$A$ is an expander. $I \in [m] : |I| < r/2$. Term $t : t \wedge [A_I x = b_I]$ is satisfiable. Then:*
*$\forall$ l.c. term $t_1$ with $|t_1| \leq k$ s.t. $d_A(Cl^e(t), t_1) > 4c^{-1}k$ the formula $t_1 \wedge t \wedge [A_I x = b_I]$ is also satisfiable.*

## Proof.

- If not then $\exists t' \in t, t'_1 \in t_1, I' \in I$ s.t. $\sum_{i \in I'}(A_i x - b_i) + \sum_{x_j^\epsilon \in t'}(x_j - \epsilon) + \sum_{x_l^\epsilon \in t'_1}(x_l - \epsilon) \equiv 1$
- We consider such $L = (I, t', t'_1)$ with minimal number of equations. $G_L$ is connected.
- $\partial(I') \subseteq Vars(t') \cup Vars(t'_1)$. $t, t_1$ are both consistent with $A_I x = b_I$, so $t, t_1$ are both non-empty.
- **Case1.** $|I' \setminus Cl^e(t)| > 2c^{-1}k$ $\left|\partial(I') \setminus \left[\bigcup_{i \in Cl^e(t)} A_i \cup Vars(t)\right]\right| \leq k \leq (c/2)|I' \setminus Cl^e(t)|$
- **Case2.** $|I' \setminus Cl^e(t)| \leq 2c^{-1}k$. Consider the minimal path in $G_L$ that connects equations, corresponding to $t$ with those corresponding to $t_1$ it goes along $I'$. Construct path of length $2|I' \setminus Cl^e(t)|$ between $t_1$ and $Cl^e(t)$ in $G(A)$.

$\square$

# Partial Assignments over Affine Subspaces

## Lemma

*Let $Y \subset X$ be a set of variables. Assume that b is a partial assignment on $Y$ uniformly distributed on some affine subspace $A \subseteq \{0,1\}^Y$. Then for any term $t$ in $Y$ variables either $Pr[t|_b \equiv 1] = 0$ or $Pr[t|_b \equiv 1] \geq 2^{-|t|}$.*

# Random Restriction

## Definition

A DNF $\phi$ is in *normal form* w.r.t. $A, b$ if each of its terms is locally consistent.

## Definition

$X = \{x_1, \ldots, x_n\}$ is the set of all variables. $D_{A,b}$ is a distribution over partial assignments over $X$ that results from the experiment:

- Choose a random $X_1 \subset X$ of size $cr/4$
- $\hat{I} = Cl^e(X_1), \quad \hat{X} = X_1 \cup \{x_j | \exists i \in \hat{I} : A_{ij} = 1\}$
- Uniformly choose $\rho$ from all $\hat{x} \in \{0,1\}^{\hat{X}}$satisfying $A_{\hat{I}}\hat{x} = b_{\hat{I}}$.

# Restriction Lemma

## Theorem

*Assume that every column of $A$ contains at most $\hat{\Delta}$ ones, $b$ is arbitrary vector and $r = \Omega(n/\hat{\Delta})$. For any $k$-DNF $\phi$ in normal form holds:*

$$Pr[\phi|_\rho \neq 1] < \left(1 - 2^{-k}\right)^{c(\phi)/\hat{\Delta}^{O(k)}}$$

## Corollary

*There exists an absolute constant $D$ s.t. under the assumption of the theorem for any normal form $k$-DNF $\phi$*

$$Pr[\phi|_\rho \neq 1] < \ 2^{-c(\phi)/\hat{\Delta}^{Dk}}$$

# Proof

## Proof.

- Observe $\hat{x} \in \{0,1\}^{\hat{X}}$ given by $\rho$.
- Assume that all bits of $\hat{x}$ are hidden. Consider a term $t_1$.
- Event $E_1$ denotes that $t_1$ is satisfied. Since $t_1$ is l.c. $Pr[E_1] \geq 2^{-k}$. If $E_1$ happens – success, otherwise:
- Step $l$: $t^{(l)}$ is a term corresponding to the partial assignment of revealed bits of $\hat{x}$. $|t^{(l)}| \leq lk$
- $Y^{(l)} \subseteq \hat{X} : d_A(Y^{(l)}, Cl^e(t^{(l)})) \leq 4c^{-1}k$
- Term $t_{l+1}$ free of these variables. If there is no – terminate, else reveal the corresponding bits.
- $Pr[E_{l+1}|t^{(l)}] \geq 2^{-k}$

$\square$

# Digression

- There are at least $C_0 = c(\phi)/k$ variable disjoint terms.
- Each of them will be covered by $X_1$ with probability at least $(cr/4n)^k$.
- The expected number of covered variable disjoint terms is $C_0(cr/4n)^k$.
- By Chernoff bound we may assume that there exist $C_1 = C_0/\hat{\Delta}^{O(k)}$ variable disjoint terms covered by $X_1$.

# Proof part 2

## Proof.

- $T$ – stopping time
- **Case 1:** $kT \leq cr/4 \quad Cl^e(t^{(T)}) \leq 2c^{-1}Tk$
- Then $|Y^{(T)}| \leq 2c^{-1}Tk\hat{\Delta}^{4c^{-1}k}$
- Since $Y^{(T)}$ is a hitting set for $\phi \quad C_1 \leq |Y^{(T)}|$ and $T \geq C_1/\hat{\Delta}^{O(k)}$
- **Case 2:** $T > cr/(4k)$. Because $r = \Omega(n/\hat{\Delta})$ and $c(\phi) \leq n$ $T \geq c(\phi)/\hat{\Delta}^{O(k)}$

$\square$

With high probability $A_{n,\Delta}$ is $(r, 0.8)$-boundary expander for some $r = \Omega(n)$.

## Definition

For matrix $A_{n,\Delta}$ let $J$ be a set of $0.2r$ columns of the largest hamming weight. $I' = Cl^e(J)$, $J' = \bigcup_{i \in I'} A_i$. By $\hat{A}_{n,\Delta}$ we denote matrix $A_{n,\Delta}$ with columns $J'$ and rows $I'$ removed. Similarly define $\hat{b}$.

## Lemma

*$\hat{A}_{n,\Delta}$ is $(r/2, 0.4)$-boundary expander in which every column has weight bounded by some $\hat{\Delta}$ that depends on $\Delta$ only.*

## Proof.

- We already proved that such matrix is either empty or $(r/2, c/2)$-boundary expander. It is not empty since $|I'| < r/2$.
- Our matrix contains at most $3\Delta n/(0.2r)$ ones in each column and $r = \Omega(n)$.

$\square$

## Lemma

*Every Res*($k$) *refutation of* $\phi_{n,\Delta}$ *can be transformed into Res*($k$) *refutation of the system* $\hat{A}_{n,\Delta}x = \hat{b}$ *in which every line is in normal form with only polynomial increase of the size.*

## Proof.

- Refutation of $\phi_{n,\Delta}$ also fits for the 3-CNF corresponding to $A_{n,\Delta}x = b$.
- We may assign values to $x_{J'}$ so that all the equations in $A_{I'}x = b_{I'}$ are satisfied. Then we get a *Res*($k$) refutation of $\hat{A}_{n,\Delta}x = \hat{b}$. Now we should transform it into a normal form.
- For every term $t$ that is not l.c. we may infer $\bar{t}$ from $2.5k$ axioms in polynomial size in *Resolution*. Thus we may substitute any occurrence of locally inconsistent terms with $\bot$ with the polynomial increase of the size of proof.

□

### Lemma(Ben-Sasson–Wigderson)

Assume that the matrix $\hat{A}_{n,\Delta}$ is $(r, c)$-boundary expander. Then every resolution refutation of the system $\hat{A}_{n,\Delta}x = \hat{b}$ requires width $\epsilon r$, where $\epsilon$ depends only on $c$.

### Theorem

*For any constant $\Delta$ with probability $1 - o(1)$ every Res$(k)$ refutation of $\phi_{n,\Delta}$ for $k < \sqrt{\log n / \log \log n}$ has size $2^{n^{1-o(1)}}$.*

# Proof of the Lower Bound

## Proof.

- If there exists *Res*($k$) refutation of $\phi_{n,\Delta}$ of size $S$ then there exists *Res*($k$) refutation $P$ of the system $\hat{A}_{n,\Delta}x = \hat{b}$ of size $Sn^{O(1)}$ which is in normal form.
- Apply restriction $\rho_{\hat{A}_{n,\Delta},b}$ constructed in the previous section to the whole refutation $P$. Due to the Corollary of Restiction Lemma for each line $F$ of $P$ $Pr[F|_\rho \neq 1] < \ 2^{-c(F)/\hat{\Delta}^{Dk}}$.
- Applying Switching Lemma plugging in parameters $d = 1, \gamma = 1, \delta = (1/\hat{\Delta})^{Dk}, s = \epsilon r/(2k)$ we have that $Pr\left[h(F|_\rho) > \epsilon r/k\right] \leq k2^{-\epsilon r(1/\hat{\Delta})^{2Dk^2}}$
- Converting Res(k) refutation to Resolution refutation we get that the restricted proof $P|_\rho$ has width less than $\epsilon r$ with probability at least $1 - Sk2^{-\epsilon r/k(1/\hat{\Delta})^{2Dk^2}} > 1 - S2^{-n/2^{O(k^2)}}$.

# The Very Last Step

## Proof.

On the other hand it is still refutation of the system which matrix is $(r/4, 0.2)$-boundary expander, so according to Ben-Sasson–Wigderson lemma the probability of this event must be 0.

At last we have $S > 2^{n/2^{O(k^2)}}$ and the theorem follows. $\square$