Circuit Complexity Minicourse: The Shrinkage Exponent of Formulas over U_2

A. S. Kulikov

http://logic.pdmi.ras.ru/~kulikov/

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R^n_m = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R^n_{\epsilon n}$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R^n_m = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R^n_{\epsilon n}$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R^n_m = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R^n_{\epsilon n}$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R^n_m = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R^n_{\epsilon n}$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R^n_m = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R^n_{\epsilon n}$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R_m^n = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R_{\epsilon n}^n$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R_m^n = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R_{\epsilon n}^n$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Random Restrictions

- a restriction is an element of $\{0, 1, *\}^n$; the interpretation of giving the value $*$ to a variable is that it remains a variable, while in the other cases the given constant is substituted as the value of the varaible
- $R_m^n = \{\rho \in \{0, 1, *\}^n : |\rho^{-1}(*)| = m\}$ is the set of all restrictions which leave exactly m variables unassigned
- choose $\rho \in R_{\epsilon n}^n$ uniformly at random
- it is easy to see that, for any basis, $E[L(f_\rho)] \leq \epsilon L(f)$ (each leaf has a probability ϵ of remainig unassigned)
- for B_2 this inequality is tight (consider the parity function)
- for U_2 however we expect more, as $\vee$ and $\wedge$ gates have the potential to be determined by one input alone
- in the following we consider the U_2 basis

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Shrinkage Exponent

- the shrinkage exponent, Γ, is the supremum of all values for which

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] = O(\epsilon^\Gamma L(f) + 1)$$

- $\Gamma \geq 1.5$ (Subbotovskaya, 61)
- $\Gamma \leq 2$ (Khrapchenko, 71)
- a function f such that $L(f) = \Omega(n^{\Gamma+1-o(1)})$ (Andreev, 87)
- $\Gamma \geq 1.55$ (Nisan and Impagliazzo, 93)
- $\Gamma \geq 1.63$ (Paterson and Zwick, 93)
- $\Gamma = 2$ (Håstad, 98)

Subbotovskaya's Lower Bound

Theorem (Subbotovskaya, 61)

If $L(f) > 1$, *then*

$$E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f) \ .$$

Proof.

- let x be any variable; by x^i we denote the i-th leaf marked by x or $\overline{x}$, by g^i_x the gate to which x_i enters and by N^i_x the other subformula that enters g^i_x; let also n_x denotes the number of leaves marked by x or $\overline{x}$ (thus, $L(f) = \sum n_x$)
- since the formula is optimal, all N^i_x are disjoint (otherwise, $N^i_x \subset N^j_x$, but in this case we can simplify the formula by assigning a value to x_i in N^j_x)
- assigning either 0 or 1 to x deletes the leaf x^i and assigning the complement value deletes both x^i and N^i_x

Subbotovskaya's Lower Bound

Theorem (Subbotovskaya, 61)

If $L(f) > 1$, *then*

$$E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f) \ .$$

Proof.

- let x be any variable; by x^i we denote the i-th leaf marked by x or $\overline{x}$, by g^i_x the gate to which x_i enters and by N^i_x the other subformula that enters g^i_x; let also n_x denotes the number of leaves marked by x or $\overline{x}$ (thus, $L(f) = \sum n_x$)
- since the formula is optimal, all N^i_x are disjoint (otherwise, $N^i_x \subset N^j_x$, but in this case we can simplify the formula by assigning a value to x_i in N^j_x)
- assigning either 0 or 1 to x deletes the leaf x^i and assigning the complement value deletes both x^i and N^i_x

Subbotovskaya's Lower Bound

Theorem (Subbotovskaya, 61)

If $L(f) > 1$, *then*

$$E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f) \ .$$

Proof.

- let x be any variable; by x^i we denote the i-th leaf marked by x or $\overline{x}$, by g^i_x the gate to which x_i enters and by N^i_x the other subformula that enters g^i_x; let also n_x denotes the number of leaves marked by x or $\overline{x}$ (thus, $L(f) = \sum n_x$)
- since the formula is optimal, all N^i_x are disjoint (otherwise, $N^i_x \subset N^j_x$, but in this case we can simplify the formula by assigning a value to x_i in N^j_x)
- assigning either 0 or 1 to x deletes the leaf x^i and assigning the complement value deletes both x^i and N^i_x

Subbotovskaya's Lower Bound

Theorem (Subbotovskaya, 61)

If $L(f) > 1$, *then*

$$E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f) \ .$$

Proof.

- let x be any variable; by x^i we denote the i-th leaf marked by x or $\overline{x}$, by g^i_x the gate to which x_i enters and by N^i_x the other subformula that enters g^i_x; let also n_x denotes the number of leaves marked by x or $\overline{x}$ (thus, $L(f) = \sum n_x$)
- since the formula is optimal, all N^i_x are disjoint (otherwise, $N^i_x \subset N^j_x$, but in this case we can simplify the formula by assigning a value to x_i in N^j_x)
- assigning either 0 or 1 to x deletes the leaf x^i and assigning the complement value deletes both x^i and N^i_x

Subbotovskaya's Lower Bound

Theorem (Subbotovskaya, 61)

If $L(f) > 1$, *then*

$$E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f) \ .$$

Proof.

- let x be any variable; by x^i we denote the i-th leaf marked by x or $\overline{x}$, by g^i_x the gate to which x_i enters and by N^i_x the other subformula that enters g^i_x; let also n_x denotes the number of leaves marked by x or $\overline{x}$ (thus, $L(f) = \sum n_x$)
- since the formula is optimal, all N^i_x are disjoint (otherwise, $N^i_x \subset N^j_x$, but in this case we can simplify the formula by assigning a value to x_i in N^j_x)
- assigning either 0 or 1 to x deletes the leaf x^i and assigning the complement value deletes both x^i and N^i_x

Proof (Cont'd)

- $(L(f) - L(f|_{x=0})) + (L(f) - L(f|_{x=1})) \geq 3n_x$
-

$$\begin{aligned} E[L(f_\rho)] &= \frac{1}{2n} \sum_{i \in [1..n]} \sum_{b \in \{0,1\}} L(f|_{x_i=b}) \\ &= L(f) - \frac{1}{2n} \sum_{i \in [1..n]} \sum_{b \in \{0,1\}} (L(f) - L(f|_{x_i=b})) \\ &= (1 - \frac{1.5}{n}) L(f) \end{aligned}$$

□

Proof (Cont'd)

- $(L(f) - L(f|_{x=0})) + (L(f) - L(f|_{x=1})) \geq 3n_x$
- $$\begin{aligned} E[L(f_\rho)] &= \frac{1}{2n} \sum_{i \in [1..n]} \sum_{b \in \{0,1\}} L(f|_{x_i=b}) \\ &= L(f) - \frac{1}{2n} \sum_{i \in [1..n]} \sum_{b \in \{0,1\}} (L(f) - L(f|_{x_i=b})) \\ &= (1 - \frac{1.5}{n}) L(f) \end{aligned}$$

Proof (Cont'd)

- $(L(f) - L(f|_{x=0})) + (L(f) - L(f|_{x=1})) \geq 3n_x$
-

$$\begin{aligned} E[L(f_\rho)] &= \frac{1}{2n} \sum_{i \in [1..n]} \sum_{b \in \{0,1\}} L(f|_{x_i=b}) \\ &= L(f) - \frac{1}{2n} \sum_{i \in [1..n]} \sum_{b \in \{0,1\}} (L(f) - L(f|_{x_i=b})) \\ &= (1 - \frac{1.5}{n}) L(f) \end{aligned}$$

□

Corollary (Subbotovskaya, 61)

$$E_{\rho \in R^n_{n-1}}[L(f_\rho) - 1/3] \leq (1 - \frac{1.5}{n})(L(f) - 1/3) \ .$$

Proof.

- if $L(f) > 1$, then the corollary follows from the previous lemma
- if $L(f) = 1$, then $E[L(f_\rho)] = 1 - 1/n$ and $(2/3 - 1/n) \leq 2/3(1 - 3/2n)$
- if $L(f) = 0$, then $-1/3 \leq -2/3(1 - 3/2n)$

□

Corollary (Subbotovskaya, 61)

$$E_{\rho \in R^n_{n-1}}[L(f_\rho) - 1/3] \leq (1 - \frac{1.5}{n})(L(f) - 1/3) \ .$$

Proof.

- if $L(f) > 1$, then the corollary follows from the previous lemma
- if $L(f) = 1$, then $E[L(f_\rho)] = 1 - 1/n$ and $(2/3 - 1/n) \leq 2/3(1 - 3/2n)$
- if $L(f) = 0$, then $-1/3 \leq -2/3(1 - 3/2n)$

Corollary (Subbotovskaya, 61)

$$E_{\rho \in R^n_{n-1}}[L(f_\rho) - 1/3] \leq (1 - \frac{1.5}{n})(L(f) - 1/3) \ .$$

Proof.

- if $L(f) > 1$, then the corollary follows from the previous lemma
- if $L(f) = 1$, then $E[L(f_\rho)] = 1 - 1/n$ and $(2/3 - 1/n) \leq 2/3(1 - 3/2n)$
- if $L(f) = 0$, then $-1/3 \leq -2/3(1 - 3/2n)$

Corollary (Subbotovskaya, 61)

$$E_{\rho \in R^n_{n-1}}[L(f_\rho) - 1/3] \leq (1 - \frac{1.5}{n})(L(f) - 1/3) \ .$$

Proof.

- if $L(f) > 1$, then the corollary follows from the previous lemma
- if $L(f) = 1$, then $E[L(f_\rho)] = 1 - 1/n$ and $(2/3 - 1/n) \leq 2/3(1 - 3/2n)$
- if $L(f) = 0$, then $-1/3 \leq -2/3(1 - 3/2n)$

Corollary (Subbotovskaya, 61)

$$E_{\rho \in R^n_{n-1}}[L(f_\rho) - 1/3] \leq (1 - \frac{1.5}{n})(L(f) - 1/3) \ .$$

Proof.

- if $L(f) > 1$, then the corollary follows from the previous lemma
- if $L(f) = 1$, then $E[L(f_\rho)] = 1 - 1/n$ and $(2/3 - 1/n) \leq 2/3(1 - 3/2n)$
- if $L(f) = 0$, then $-1/3 \leq -2/3(1 - 3/2n)$

□

Lemma

For any $a \geq 1$ and $m \leq n$,

$$\prod_{k=m+1}^{n} (1 - \frac{a}{k}) \leq \left(\frac{m}{n}\right)^a \quad .$$

Proof.

- $(1 - a/k) \leq (1 - 1/k)^a$
- $\prod_{k=m+1}^{n}(1 - 1/k) = m/n$

□

Lemma

For any $a \geq 1$ and $m \leq n$,

$$\prod_{k=m+1}^{n} (1 - \frac{a}{k}) \leq \left(\frac{m}{n}\right)^a \quad .$$

Proof.

- $(1 - a/k) \leq (1 - 1/k)^a$
- $\prod_{k=m+1}^{n}(1 - 1/k) = m/n$

Lemma

For any $a \geq 1$ and $m \leq n$,

$$\prod_{k=m+1}^{n} (1 - \frac{a}{k}) \leq \left(\frac{m}{n}\right)^a \quad .$$

Proof.

- $(1 - a/k) \leq (1 - 1/k)^a$
- $\prod_{k=m+1}^{n}(1 - 1/k) = m/n$

Lemma

For any $a \geq 1$ and $m \leq n$,

$$\prod_{k=m+1}^{n} (1 - \frac{a}{k}) \leq \left(\frac{m}{n}\right)^a \quad .$$

Proof.

- $(1 - a/k) \leq (1 - 1/k)^a$
- $\prod_{k=m+1}^{n}(1 - 1/k) = m/n$

□

Theorem (Subbotovskaya, 61)

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] \leq \epsilon^{1.5} L(f) + 1/3 \ .$$

Proof.

- construct a random sequence of functions $f_n = f, f_{n-1}, \ldots, f_m$ $(m = \epsilon n)$, where f_i is obtained from f_{i+1} by assigning a random value to a random variable
- $E[L(f_k) - 1/3] \leq (1 - \frac{1.5}{k+1}) E[L(f_{k+1}) - 1/3]$
-

$$\begin{aligned} E[L(f_m) - 1/3] &\leq \left(\prod_{k=m+1}^{n} 1 - \frac{1.5}{k} \right) (L(f) - 1/3) \\ &\leq \epsilon^{1.5} (L(f) - 1/3) \end{aligned}$$

□

Theorem (Subbotovskaya, 61)

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] \leq \epsilon^{1.5} L(f) + 1/3 \ .$$

Proof.

- construct a random sequence of functions $f_n = f, f_{n-1}, \ldots, f_m$ $(m = \epsilon n)$, where f_i is obtained from f_{i+1} by assigning a random value to a random variable
- $E[L(f_k) - 1/3] \leq (1 - \frac{1.5}{k+1}) E[L(f_{k+1}) - 1/3]$
-

$$\begin{aligned} E[L(f_m) - 1/3] &\leq \left(\prod_{k=m+1}^{n} 1 - \frac{1.5}{k} \right) (L(f) - 1/3) \\ &\leq \epsilon^{1.5} (L(f) - 1/3) \end{aligned}$$

□

Theorem (Subbotovskaya, 61)

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] \leq \epsilon^{1.5} L(f) + 1/3 \ .$$

Proof.

- construct a random sequence of functions $f_n = f, f_{n-1}, \ldots, f_m$ $(m = \epsilon n)$, where f_i is obtained from f_{i+1} by assigning a random value to a random variable
- $E[L(f_k) - 1/3] \leq (1 - \frac{1.5}{k+1}) E[L(f_{k+1}) - 1/3]$
-

$$\begin{aligned} E[L(f_m) - 1/3] &\leq \left(\prod_{k=m+1}^{n} 1 - \frac{1.5}{k} \right) (L(f) - 1/3) \\ &\leq \epsilon^{1.5} (L(f) - 1/3) \end{aligned}$$

□

Theorem (Subbotovskaya, 61)

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] \leq \epsilon^{1.5} L(f) + 1/3 \ .$$

Proof.

- construct a random sequence of functions $f_n = f, f_{n-1}, \ldots, f_m$ $(m = \epsilon n)$, where f_i is obtained from f_{i+1} by assigning a random value to a random variable
- $E[L(f_k) - 1/3] \leq (1 - \frac{1.5}{k+1}) E[L(f_{k+1}) - 1/3]$
-

$$\begin{aligned} E[L(f_m) - 1/3] &\leq \left(\prod_{k=m+1}^{n} 1 - \frac{1.5}{k} \right) (L(f) - 1/3) \\ &\leq \epsilon^{1.5} (L(f) - 1/3) \end{aligned}$$

□

Theorem (Subbotovskaya, 61)

$$E_{\rho \in R^n_{\epsilon n}}[L(f_\rho)] \leq \epsilon^{1.5} L(f) + 1/3 \ .$$

Proof.

- construct a random sequence of functions $f_n = f, f_{n-1}, \ldots, f_m$ $(m = \epsilon n)$, where f_i is obtained from f_{i+1} by assigning a random value to a random variable
- $E[L(f_k) - 1/3] \leq (1 - \frac{1.5}{k+1}) E[L(f_{k+1}) - 1/3]$
-

$$\begin{aligned} E[L(f_m) - 1/3] &\leq \left(\prod_{k=m+1}^{n} 1 - \frac{1.5}{k} \right) (L(f) - 1/3) \\ &\leq \epsilon^{1.5} (L(f) - 1/3) \end{aligned}$$

□

$\Omega(n^{1.5})$ Bound for Parity

Theorem

$$L(\mathit{parity}) = \Omega(n^{1.5}) \ .$$

Proof.

- $f = \mathit{parity}_n$
- $E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f)$
- in particular, there is a variable x_i and a value b such that $L(f|_{x_i=b}) \leq (1 - \frac{1.5}{n})L(f)$
- since $f|_{x_i=b}$ is either parity_n or $\overline{\mathit{parity}_n}$, then

$$L(f_{n-1}) \leq (1 - \frac{1.5}{n})L(f_n)$$

- hence $L(\mathit{parity}_n) \geq n^{1.5} L(\mathit{parity}_1) = n^{1.5}$

$\Omega(n^{1.5})$ Bound for Parity

Theorem

$$L(\mathit{parity}) = \Omega(n^{1.5}) \ .$$

Proof.

- $f = \mathit{parity}_n$
- $E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f)$
- in particular, there is a variable x_i and a value b such that $L(f|_{x_i=b}) \leq (1 - \frac{1.5}{n})L(f)$
- since $f|_{x_i=b}$ is either parity_n or $\overline{\mathit{parity}_n}$, then

$$L(f_{n-1}) \leq (1 - \frac{1.5}{n})L(f_n)$$

- hence $L(\mathit{parity}_n) \geq n^{1.5} L(\mathit{parity}_1) = n^{1.5}$

$\Omega(n^{1.5})$ Bound for Parity

Theorem

$$L(\mathit{parity}) = \Omega(n^{1.5}) \ .$$

Proof.

- $f = \mathit{parity}_n$
- $E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f)$
- in particular, there is a variable x_i and a value b such that $L(f|_{x_i=b}) \leq (1 - \frac{1.5}{n})L(f)$
- since $f|_{x_i=b}$ is either parity_n or $\overline{\mathit{parity}_n}$, then

$$L(f_{n-1}) \leq (1 - \frac{1.5}{n})L(f_n)$$

- hence $L(\mathit{parity}_n) \geq n^{1.5} L(\mathit{parity}_1) = n^{1.5}$

$\Omega(n^{1.5})$ Bound for Parity

Theorem

$$L(parity) = \Omega(n^{1.5}) \ .$$

Proof.

- $f = parity_n$
- $E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f)$
- in particular, there is a variable x_i and a value b such that $L(f|_{x_i=b}) \leq (1 - \frac{1.5}{n})L(f)$
- since $f|_{x_i=b}$ is either $parity_n$ or $\overline{parity_n}$, then

$$L(f_{n-1}) \leq (1 - \frac{1.5}{n})L(f_n)$$

- hence $L(parity_n) \geq n^{1.5} L(parity_1) = n^{1.5}$

$\Omega(n^{1.5})$ Bound for Parity

Theorem

$$L(\mathit{parity}) = \Omega(n^{1.5}) \ .$$

Proof.

- $f = \mathit{parity}_n$
- $E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f)$
- in particular, there is a variable x_i and a value b such that $L(f|_{x_i=b}) \leq (1 - \frac{1.5}{n})L(f)$
- since $f|_{x_i=b}$ is either parity_n or $\overline{\mathit{parity}_n}$, then

$$L(f_{n-1}) \leq (1 - \frac{1.5}{n})L(f_n)$$

- hence $L(\mathit{parity}_n) \geq n^{1.5} L(\mathit{parity}_1) = n^{1.5}$

$\Omega(n^{1.5})$ Bound for Parity

Theorem

$$L(parity) = \Omega(n^{1.5}) \ .$$

Proof.

- $f = parity_n$
- $E_{\rho \in R^n_{n-1}}[L(f_\rho)] \leq (1 - \frac{1.5}{n})L(f)$
- in particular, there is a variable x_i and a value b such that $L(f|_{x_i=b}) \leq (1 - \frac{1.5}{n})L(f)$
- since $f|_{x_i=b}$ is either $parity_n$ or $\overline{parity_n}$, then

$$L(f_{n-1}) \leq (1 - \frac{1.5}{n})L(f_n)$$

- hence $L(parity_n) \geq n^{1.5} L(parity_1) = n^{1.5}$

□

Andreev's Function

$$A_n(x, y) = Y_{\sum_{i=0}^{\log n - 1} \left(\bigoplus_{j=1}^{n/\log n} x_{ij} \right) 2^i}$$

$|x| = |y| = n$. The bits of x are organized into $\log n$ rows of $n/\log n$ bits each. The function first computes the parity of the bits in each row and then uses the obtained $\log n$-bit number to index into the array y.

Theorem (Andreev, 85)

$$L(A_n) = \Omega(n^{2.5 - o(1)}) \ .$$

Andreev's Function

$$A_n(x, y) = Y_{\sum_{i=0}^{\log n - 1} \left(\bigoplus_{j=1}^{n/\log n} x_{ij} \right) 2^i}$$

$|x| = |y| = n$. The bits of x are organized into $\log n$ rows of $n/\log n$ bits each. The function first computes the parity of the bits in each row and then uses the obtained $\log n$-bit number to index into the array y.

Theorem (Andreev, 85)

$$L(A_n) = \Omega(n^{2.5 - o(1)}) \ .$$

Andreev's Function

$$A_n(x, y) = Y_{\sum_{i=0}^{\log n - 1} \left(\bigoplus_{j=1}^{n/\log n} x_{ij} \right) 2^i}$$

$|x| = |y| = n$. The bits of x are organized into $\log n$ rows of $n/\log n$ bits each. The function first computes the parity of the bits in each row and then uses the obtained $\log n$-bit number to index into the array y.

Theorem (Andreev, 85)

$$L(A_n) = \Omega(n^{2.5 - o(1)}) \ .$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof

- using counting arguments, Shannon showed that there exists a function f on $\log n$ variables whose formula complexity is at least $n/\log\log n$
- let y^* be the truth table for f and consider the function $A^*(x) = A(x, y^*)$
- hit A^* with a random restriction that leaves only $m = 2\log n \log\log n$ variables
- when n is large enough, with probability $> 1/2$ there will be at least one free variable in each row of x and in this case $L(A_\rho) \geq L(f) \geq n/\log\log n$
- consider the probability that none of the variables in the first row remains unrestricted
- the probability that one of unassigned variables is not in the first row is $(1 - 1/\log n)$
- the probability that none of them is in the first row is at most

$$(1 - \frac{1}{\log n})^m < 2^{-\frac{m}{\log n}} = \frac{1}{\log^2 n}$$

Proof (Cont'd)

- the probability that some row has no free variables is at most

$$\log n \left(\frac{1}{\log^2 n} \right)$$

- with probability at least $1/2$ every row contains an unassigned variable
- $$\frac{1}{2} n / \log \log n \leq E_{\rho \in R_m^n}[L(A^*)] \leq \left(\frac{m}{n} \right)^{1.5} L(A^*) + \frac{1}{3}$$

- $$L(A) \geq L(A^*) = \Omega \left(\frac{n^{2.5}}{\log^{1.5} n (\log \log n)^{2.5}} \right)$$

□

Proof (Cont'd)

- the probability that some row has no free variables is at most

$$\log n \left(\frac{1}{\log^2 n} \right)$$

- with probability at least $1/2$ every row contains an unassigned variable
- $$\frac{1}{2} n / \log \log n \leq E_{\rho \in R_m^n}[L(A^*)] \leq \left(\frac{m}{n} \right)^{1.5} L(A^*) + \frac{1}{3}$$
- $$L(A) \geq L(A^*) = \Omega \left(\frac{n^{2.5}}{\log^{1.5} n (\log \log n)^{2.5}} \right)$$

□

Proof (Cont'd)

- the probability that some row has no free variables is at most

$$\log n \left(\frac{1}{\log^2 n} \right)$$

- with probability at least $1/2$ every row contains an unassigned variable
- $$\frac{1}{2} n / \log \log n \leq E_{\rho \in R_m^n}[L(A^*)] \leq \left(\frac{m}{n} \right)^{1.5} L(A^*) + \frac{1}{3}$$
- $$L(A) \geq L(A^*) = \Omega \left(\frac{n^{2.5}}{\log^{1.5} n (\log \log n)^{2.5}} \right)$$

□

Proof (Cont'd)

- the probability that some row has no free variables is at most

$$\log n \left(\frac{1}{\log^2 n} \right)$$

- with probability at least $1/2$ every row contains an unassigned variable
-

$$\frac{1}{2} n / \log \log n \leq E_{\rho \in R_m^n}[L(A^*)] \leq \left(\frac{m}{n} \right)^{1.5} L(A^*) + \frac{1}{3}$$

-

$$L(A) \geq L(A^*) = \Omega \left(\frac{n^{2.5}}{\log^{1.5} n (\log \log n)^{2.5}} \right)$$

□

Proof (Cont'd)

- the probability that some row has no free variables is at most

$$\log n \left(\frac{1}{\log^2 n} \right)$$

- with probability at least $1/2$ every row contains an unassigned variable
- $$\frac{1}{2} n / \log \log n \leq E_{\rho \in R_m^n}[L(A^*)] \leq \left(\frac{m}{n} \right)^{1.5} L(A^*) + \frac{1}{3}$$

- $$L(A) \geq L(A^*) = \Omega \left(\frac{n^{2.5}}{\log^{1.5} n (\log \log n)^{2.5}} \right)$$

□