Strong Direct Sum for Randomized Query Complexity

Eric Blais  
University of Waterloo

Joshua Brody  
Swarthmore College

Conference on Computational Complexity  
New Brunswick, New Jersey  
July 18, 2019
Outline

• Introduction
• Strong Direct Sum
• Query Resistance
• Separation Theorem
• Open Problems
Direct Sum Theorems

Does computing $f(x)$ on $k$ copies scale with $k$?
Direct Sum Theorems

Does computing $f(x)$ on $k$ copies scale with $k$?

Direct Sum Theorem: Computing $k$ copies of $f$ requires $k$ times the resources.

Direct Product Theorem: Success prob. of computing $k$ copies of $f$ with $<< k$ resources is $2^{-Ω(k)}$.
Direct Sum Theorems

Does computing $f(x)$ on $k$ copies scale with $k$?

Direct Sum Theorem: Computing $k$ copies of $f$ requires $k$ times the resources.

Direct Product Theorem: Success prob. of computing $k$ copies of $f$ with $\ll k$ resources is $2^{-\Omega(k)}$.

Strong Direct Sum: computing $k$ copies of $f$ w/error $\varepsilon$ requires $\gg k$ times the resources.
Our Main Results

Strong Direct Sum for average query complexity:
For any $f$ and any $k$, computing $f^k$ satisfies:
\[ \bar{R}_\varepsilon(f^k) = \Theta(k \bar{R}_{\varepsilon/k}(f)) \]

Separation Theorem: for all $\varepsilon > 2^{-n^{1/3}}$, there is total function $f : \{0,1\}^n \to \{0,1\}$ such that $\bar{R}_\varepsilon(f) = \Theta(R(f) \log(1/\varepsilon))$

Corollary: There is $f$ such that $R_\varepsilon(f^k) = \Theta(k \log(k) R_\varepsilon(f))$
Query Complexity

aka Decision Tree Complexity
Query Complexity

aka Decision Tree Complexity

Decision Tree for \( f: \{0,1\}^n \rightarrow \{0,1\} \):

- internal nodes labeled w/input bits \( x_i \)
- leaves labeled w/output or \text{ABORT}
- \( \text{cost}(T,x) \): depth of \( T \) on input \( x \)

Randomized DT: distribution \( A \) on decision trees

- \( \text{cost}(A) = \max_{T,x} \text{cost}(T,x) \)
- \( \text{acost}(A) = \max_x E_{T \sim A} [\text{cost}(T, x)] \)
Query Complexity

*aka Decision Tree Complexity*

Decision Tree for \( f: \{0,1\}^n \rightarrow \{0,1\} \):
- internal nodes labeled w/input bits \( x_i \)
- leaves labeled w/output or ABORT
- \( \text{cost}(T,x) \): depth of \( T \) on input \( x \)

Randomized DT: distribution \( A \) on decision trees
- \( \text{cost}(A) = \max_{T,x} \text{cost}(T,x) \)
- \( \text{acost}(A) = \max_x \mathbb{E}_{T \sim A} [\text{cost}(T, x)] \)

Distributional QC \( D^u_{\delta,\varepsilon}(f) \): \[ \min \mathbb{E}_x[\text{cost}(T,x)] \text{ s.t. } \Pr[\text{abort}] \leq \delta \text{ and } \Pr[\text{error}] \leq \varepsilon \]

Randomized QC \( R_{\delta,\varepsilon}(f) \): minimum cost of randomized algorithm s.t.
\[ \Pr[\text{abort}] \leq \delta \text{ and } \Pr[\text{error}] \leq \varepsilon \]

Average case Randomized QC \( \bar{R}_{\varepsilon}(f) \):
minimum acost of randomized algorithm s.t. \( \Pr[\text{error}] \leq \varepsilon \)
Basic Results

**Minimax Lemma:** \( \max_{\mu} D_{2\delta,2\varepsilon}^{\mu}(f) \leq R_{\delta,\varepsilon}(f) \leq \max_{\mu} D_{\delta/2,\varepsilon/2}^{\mu}(f) \)

**Error Reduction:** \( R_{o(1/t), o(1/t)}(f) \leq O(\log(t) R_{1/2, 1/3}(f)) \)

**Average QC vs Aborts:** \( \delta R_{\delta,\varepsilon}(f) \leq \bar{R}_{\varepsilon}(f) \leq R_{\delta,(1-\delta)\varepsilon}(f)/(1-\delta) \)
Basic Results

Average QC vs Aborts: \( \delta R_{\delta,\varepsilon}(f) \leq \tilde{R}_\varepsilon(f) \leq R_{\delta,(1-\delta)\varepsilon}(f)/(1-\delta) \)

First inequality:
Algorithm \( A \): \( \varepsilon \)-error,
\( \text{acost}(A) = q \)

Second inequality:
Algorithm \( B' \): \( (1-\delta)\varepsilon \)-error,
\( \delta \)-abort, \( q \) queries.
Basic Results

Average QC vs Aborts: \( \delta R_{\delta, \varepsilon}(f) \leq \bar{R}_\varepsilon(f) \leq R_{\delta, (1-\delta)\varepsilon}(f)/(1-\delta) \)

First inequality:
Algorithm \( A \): \( \varepsilon \)-error,
\[ \text{acost}(A) = q \]

Algorithm \( B(x) \) {
  emulate \( A(x) \)
  abort if > \( q/\delta \) queries
}

Second inequality:
Algorithm \( B' \): \( (1-\delta)\varepsilon \)-error,
\( \delta \)-abort, \( q \) queries.

Algorithm \( A'(x) \) {
  repeat:
  emulate \( B'(x) \)
  until no aborts
}
Previous Work

Information Complexity: [MWY13, MWY15]
- strong direct sum for information complexity w/aborts + error
- applications for streaming/sketching algorithms

Direct Product Theorem: [Drucker 12]
- direct product theorems for randomized query complexity

Separation Theorems: [GPW15, ABBLSS17]
- query complexity separations based on pointer functions
- polynomial separation $R_0(f)$ vs $R_\varepsilon(f)$

Direct Sum Theorems:
- [Jain Klauck Santha 10]: $R_\varepsilon(f^k) \geq \delta^2 k R_\varepsilon/(1-\delta) + \delta(f)$
- [Ben-David Kothari 18]: $\overline{R}_\varepsilon(f^k) \geq k \overline{R}_\varepsilon(f)$
Our Results

**Strong Direct Sum Theorem:** \( D_{0,\varepsilon}^{\mu}(f^k) = \Omega(kD_{1/5,40\varepsilon/k}(f)) \)

**Separation Theorem:** There is \( f : \{0,1\}^N \rightarrow \{0,1\} \) such that for all \( \varepsilon > 2^{-N^{1/3}} \), we have \( R_{\delta,\varepsilon}(f) = \Omega(R_{1/3}(f)\log(1/\varepsilon)) \)

**Corollary:** There is \( f \) such that \( R_{1/3}(f^k) = \Omega(k\log(k)R_{\varepsilon}(f)) \)
Our Results

**Strong Direct Sum Theorem:** \[ D_{0, \varepsilon}^{\mu k}(f^k) = \Omega(k D_{1/5, 4\varepsilon/k}^{\mu}(f)) \]

**Separation Theorem:** There is \( f : \{0,1\}^N \rightarrow \{0,1\} \) such that for all \( \varepsilon > 2^{-N^{1/3}} \), we have \( R_{\delta, \varepsilon}(f) = \Omega(R_{1/3}(f) \log(1/\varepsilon)) \)

**Corollary:** There is \( f \) such that \( R_{1/3}(f^k) = \Omega(k \log(k) R_{\varepsilon}(f)) \)

**proof:** \[ R_{1/3}(f^k) \geq R_{0,1/3}(f^k) = \Omega(k R_{1/5,40/3k}(f)) = \Omega(k \log(k) R_{1/3}(f)) \]
Our Results

**Strong Direct Sum Theorem:**  \[ D_{0,\varepsilon}^\mu(f^k) = \Omega(kD_{1/5,40}\varepsilon/k(f)) \]

**Separation Theorem:**  There is \( f : \{0,1\}^N \rightarrow \{0,1\} \) such that for all \( \varepsilon > 2^{-N^{1/3}} \), we have \( R_{\delta,\varepsilon}(f) = \Omega(R_{1/3}(f)\log(1/\varepsilon)) \)

**Corollary:**  There is \( f \) such that \( R_{1/3}(f^k) = \Omega(k\log(k)R_{\varepsilon}(f)) \)

**proof:**  \( R_{1/3}(f^k) \geq R_{0,1/3}(f^k) = \Omega(kR_{1/5,40/3k}(f)) = \Omega(k\log(k)R_{1/3}(f)) \)

**Key Technical result:**

**Query-resistant codes:**  probabilistic encoding \( G: \Sigma \rightarrow \{0,1\}^N \) such that \( N/3 \) bits of \( G(x) \) needed to learn anything about \( x \)
Outline

• Introduction
• Strong Direct Sum
• Query Resistance
• Separation Theorem
• Open Problems
Strong Direct Sum Theorem: \( D_{0,\varepsilon}(f^k) = \Omega(kD_{1/5,40\varepsilon/k}(f)) \)

Let \( A \) be an \( \varepsilon \)-error algorithm for \( f^k \) with \( q \) queries.

Goal: \( (\varepsilon/k) \)-error algorithm \( B \) for \( f \) with \( q/k \) queries.

Let \( y = (y_1, \ldots, y_k) \).

\textbf{Embed}(y, i, x) := y, \text{ w/i-th coord replaced by } x.
Strong Direct Sum Theorem: \( D_{0,\epsilon}(f^k) = \Omega(kD_{1/5,40\epsilon/k}(f)) \)

Let \( A \) be an \( \epsilon \)-error algorithm for \( f^k \) with \( q \) queries.  
Goal: \((\epsilon/k)\)-error algorithm \( B \) for \( f \) with \( q/k \) queries.  
Let \( y = (y_1, \ldots, y_k) \).  
\( \text{Embed}(y,i,x) := y, \) w/i-th coord replaced by \( x \).  

```
Algorithm B(x) {
    carefully select y,i
    emulate A(Embed(y,i,x))
    abort if problems found
}
```
Strong Direct Sum Theorem: \( D_{0,\varepsilon}^k(f^k) = \Omega(kD_{1/5,40\varepsilon/k}^\mu(f)) \)

Let \( A \) be an \( \varepsilon \)-error algorithm for \( f^k \) with \( q \) queries.  
Goal: \( (\varepsilon/k) \)-error algorithm \( B \) for \( f \) with \( q/k \) queries. 
Let \( y = (y_1, \ldots, y_k) \). 
\( \text{Embed}(y,i,x) := y, \text{w/i-th coord replaced by } x. \) 

Algorithm \( B(x) \)  
{  
carefully select \( y,i \)  
emulate \( A(\text{Embed}(y,i,x)) \)  
abort if problems found  
}

Intuition: success on typical coordinate \( \geq 1 - 10\varepsilon/k \) 
else overall success \( < (1 - 10\varepsilon/k)^k < 1 - \varepsilon \)
Strong Direct Sum Theorem: \( D_{0,\varepsilon}^{\mu}(f^k) = \Omega(kD_{1/5,40\varepsilon/k}(f)) \)

\[
1 - \varepsilon \leq \Pr_{Y \sim \mu^k}[A(Y) = f^k(Y)] = \prod_{i=1}^{k} \Pr_{Y \sim \mu^k}[A(Y)_i = f^k(Y)_i \mid A(Y)_{<i} = f^k(Y)_{<i}]
\]
Strong Direct Sum Theorem: \( D_{0,\varepsilon}(f^k) = \Omega(kD_{1/5,40\varepsilon/k}(f)) \)

\[
1 - \varepsilon \leq \Pr_{Y \sim \mu^k}[A(Y) = f^k(Y)] = \prod_{i=1}^{k} \Pr_{Y \sim \mu^k}[A(Y)_i = f^k(Y)_i | A(Y)_{<i} = f^k(Y)_{<i}]
\]

Want: \( i \) such that

1. (1) conditional error very low:
   \[
   \Pr[A \text{ err. on } i\text{-th coord.} | \text{correct on } < i] \leq 10 \varepsilon/k
   \]

2. (2) Expected # queries on i-th coord not too high:
   \[
   E[\text{queries on } i\text{-th coord.}] \leq 3q/k
   \]
Strong Direct Sum Theorem: \( D_{0,\varepsilon}^{\mu k}(f^k) = \Omega(k D_{1/5,40\varepsilon/k}^{\mu}(f)) \)

\[
1 - \varepsilon \leq \Pr_{Y \sim \mu^k} [A(Y) = f^k(Y)] = \prod_{i=1}^k \Pr_{Y \sim \mu^k} [A(Y)_i = f^k(Y)_i \mid A(Y)_{<i} = f^k(Y)_{<i}]
\]

Want: \( i \) such that

1. Conditional error very low:
   \( \Pr[A \text{ err. on } i\text{-th coord.} \mid \text{correct on } < i] \leq 10 \varepsilon/k \)

2. Expected # queries on i-th coord not too high:
   \( \mathbb{E}[\text{queries on } i\text{-th coord.}] \leq 3q/k \)

Fact: at least \( \frac{2k}{3} \) coords. satisfy (1)

Fact: at least \( \frac{2k}{3} \) coords. satisfy (2)

\( \implies \) There is \( i^* \) satisfying (1) and (2). \( Y^* := \text{Embed}(Y, i^*, x) \).
Strong Direct Sum Theorem: \( D_{0,\varepsilon}^{\mu,k}(f^k) = \Omega(kD_1^{\mu,1/5,40\varepsilon/k}(f)) \)

This \( i^* \) satisfies:

1. \( E_{Y \sim \mu^k}[ \Pr_{x \sim \mu}[A(Y^*)_i \neq f^k(Y^*)_i] ] \leq \varepsilon \)

2. \( E_{Y \sim \mu^k}[\Pr_{x \sim \mu}[A(Y^*)_i \neq f^k(Y^*)_i \mid A(Y^*)_i = f^k(Y^*)_i] \] \( \leq 10 \varepsilon/k \)

3. \( E_{Y \sim \mu^k}[ E_X[q_{i^*}(Y^*)] ] \leq 3q/k \)
Strong Direct Sum Theorem:  \[ D_{0, \varepsilon}^\mu(f^k) = \Omega(kD_{1/5, 40\varepsilon/k}(f)) \]

This \( i^* \) satisfies:

1. \( E_{Y \sim \mu^k}[ \Pr_{x \sim \mu}[A(Y^*)_{<i^*} \neq f^k(Y^*)_{<i^*}] ] \leq \varepsilon \)
2. \( E_{Y \sim \mu^k}[\Pr_{x \sim \mu}[A(Y^*)_{i^*} \neq f^k(Y^*)_{i^*} \mid A(Y^*)_{<i^*} = f^k(Y^*)_{<i^*}] \leq 10 \varepsilon/k \)
3. \( E_{Y \sim \mu^k}[E_x[q_{i^*}(Y^*)]] \leq 3q/k \)

Markov Inequality: there is \( y^* \) such that

1. \( \Pr_{x \sim \mu}[A(Y^*)_{<i^*} \neq f^k(Y^*)_{<i^*}] \leq 4\varepsilon \)
2. \( \Pr_{x \sim \mu}[A(Y^*)_{i^*} \neq f^k(Y^*)_{i^*} \mid A(Y^*)_{<i^*} = f^k(Y^*)_{<i^*}] \leq 40 \varepsilon/k \)
3. \( E_x[q_{i^*}(Y^*)] \leq 12q/k \)
Algorithm B(x) {
    z := EMBED(y*,i*,x)
    emulate A(z)
    abort if \( q_{i^*}(z) > 120q/k \)
    abort if \( A(z)_{<i^*} \neq f^k(z)_{<i^*} \)
}

**Strong Direct Sum Theorem:** \( D_{0,\epsilon}(f^k) = \Omega(kD_{1/5,40\epsilon/k}(f)) \)

This \( i^* \) satisfies:

1. \( \mathbb{E}_{Y \sim \mu^k}[ \Pr_{x \sim \mu}[A(Y^*)_{<i^*} \neq f^k(Y^*)_{<i^*}] ] \leq \epsilon \)
2. \( \mathbb{E}_{Y \sim \mu^k}[\Pr_{x \sim \mu}[A(Y^*)_{i^*} \neq f^k(Y^*)_{i^*} | A(Y^*)_{<i^*} = f^k(Y^*)_{<i^*}] \leq 10 \frac{\epsilon}{k} \)
3. \( \mathbb{E}_{Y \sim \mu^k}[ \mathbb{E}_{X}[q_{i^*}(Y^*)] ] \leq 3q/k \)

**Markov Inequality:** there is \( y^* \) such that

1. \( \Pr_{x \sim \mu}[A(Y^*)_{<i^*} \neq f^k(Y^*)_{<i^*}] \leq 4\epsilon \)
2. \( \Pr_{x \sim \mu}[A(Y^*)_{i^*} \neq f^k(Y^*)_{i^*} | A(Y^*)_{<i^*} = f^k(Y^*)_{<i^*}] \leq 40 \frac{\epsilon}{k} \)
3. \( \mathbb{E}_{X}[q_{i^*}(Y^*)] \leq 12q/k \)
Algorithm B(x) {
  z := EMBED(y*,i*,x)
  emulate A(z)
  abort if q_{i*}(z) > 120q/k
  abort if A(z)_{i*} ≠ f^k(z)_{i*}
}

Strong Direct Sum Theorem: \( D_{0, \varepsilon}(f^k) = \Omega(kD_{1/5, 40\varepsilon/k}(f)) \)

This \( i^* \) satisfies:
1. \( E_{Y \sim \mu^k}[ \Pr_{x \sim \mu}[A(Y^*)_{i^*} ≠ f^k(Y^*)_{i^*}] ] ≤ \varepsilon \)
2. \( E_{Y \sim \mu^k}[\Pr_{x \sim \mu}[A(Y^*)_{i^*} ≠ f^k(Y^*)_{i^*} | A(Y^*)_{i^*} = f^k(Y^*)_{i^*}] ] ≤ 10 \frac{\varepsilon}{k} \)
3. \( E_{Y \sim \mu^k}[E_X[q_{i^*}(Y^*)]] ] ≤ 3q/k \)

Markov Inequality: there is \( y^* \) such that
1. \( \Pr_{x \sim \mu}[A(Y^*)_{i^*} ≠ f^k(Y^*)_{i^*}] ≤ 4\varepsilon \)
2. \( \Pr_{x \sim \mu}[A(Y^*)_{i^*} ≠ f^k(Y^*)_{i^*} | A(Y^*)_{i^*} = f^k(Y^*)_{i^*}] ≤ 40 \frac{\varepsilon}{k} \)
3. \( E_X[q_{i^*}(Y^*)] ≤ 12q/k \)

Abort probability: \( \frac{1}{10} + 4\varepsilon < \frac{1}{5} \)
Error probability: \( 40\varepsilon/k \)
Outline

• Introduction
• Strong Direct Sum
• **Query Resistance**
• Separation Theorem
• Open Problems
**Pointer Function**

\[ \text{PtrFcn}: \Sigma^{n \times n} \rightarrow \{0,1\} \]

each cell \( z \in \Sigma \) has:
- value \( b \in \{0,1\} \)
- \( n \) row ptrs \( \text{row}_1(z), \ldots, \text{row}_n(z) \)
- back ptr \( \text{back}(z) \)

\[ \text{PtrFcn}(X) := 1 \text{ iff } \]
- \( \exists \) unique col \( j^* \): \( \text{val}(z_{i,j^*}) = 1 \) for all \( i \).
- \( \exists \) special cell \( z_{i^*,j^*} \). all ptrs \textbf{NULL} in col \( j^* \) except for special cell
- special cell pts to \textbf{0}-value \textit{linked cells} in each other col
- exactly half of \textit{linked cells} point back to \textit{special cell}

[GPW15, ABBLSS17, BB19]
Query Resistant Codes

**Definition:** a $\delta N$-query resistant code of $\Sigma$ is a set of distribs $\{G(x)\}$

- For each $x \in \Sigma$, $G(x)$ is a distribution on $\{0,1\}^N$
- $\{\text{support}(G(x)) : x \in \Sigma\}$ partition $\{0,1\}^N$
- For all $S \subseteq [N]$ with $|S| \leq \delta N$, distributions $G(x)|_S = G(x')|_S$
- “decoding function” $h(y) := x$ iff $y \in \text{support}(G(x))$
**Definition:** a $\delta N$-query resistant code of $\Sigma$ is a set of distributions $\{G(x)\}$

- For each $x \in \Sigma$, $G(x)$ is a distribution on $\{0,1\}^N$
- $\{\text{support}(G(x)) : x \in \Sigma\}$ partition $\{0,1\}^N$
- For all $S \subseteq [N]$ with $|S| \leq \delta N$, distributions $G(x)|_S = G(x')|_S$
- “decoding function” $h(y) := x$ iff $y \in \text{support}(G(x))$

**Theorem:** [Chor et al. 85] For any $\Sigma$, there is a $(N/3)$-query resistant code with $N = 12.5 \log(|\Sigma|)$. Furthermore, conditional distributions $G(x)|_S$ are uniform.
For $f : \Sigma^n \rightarrow \{0,1\}$, define $F : \{0,1\}^{nN} \rightarrow \{0,1\}$ as:

$$F(y_1,\ldots,y_n) := f(h(y_1),\ldots,h(y_n))$$

**Theorem:** $R_{\delta,\epsilon}(f) \leq (3/N)R_{\delta,\epsilon}(F)$
Query Resistance

For $f : \Sigma^n \rightarrow \{0,1\}$, define $F : \{0,1\}^{nN} \rightarrow \{0,1\}$ as:

$$F(y_1,\ldots,y_n) := f(h(y_1),\ldots, h(y_n))$$

**Theorem:** $R_{\delta,\varepsilon}(f) \leq (3/N)R_{\delta,\varepsilon}(F)$

**Proof:** Let $A$ be a $(q, \delta, \varepsilon)$-algorithm for $F$.

**Algorithm** $B(x_1,\ldots, x_n)$ {
    
    emulate $A(G(x_1),\ldots, G(x_n))$
    
    when $A$ queries $G(x_i)$ for $k$-th time:
    
    if $k < N/3$, sample $G(x_i)$ cond. on prev. queries
    
    if $k = N/3$, sample $x_i$
    
    if $k \geq N/3$, sample $G(x_i)$ cond. on prev. history.

}
Open Problems

1. *Characterize* functions robust to **aborts**

2. **Strong Direct Sum** for Composed Functions
   (a) XOR Lemma
   (b) Strong Direct Sum for MAJ

3. How does $R_{\delta,\varepsilon}(f)$ compare to other QC measures?
Thanks!

NOTE: Swarthmore has a tenure-track opening for fall 2020!