Advanced Algorithms (VIII)

Yijia Chen
Fudan University
Review
Definition
An $n$-variable algebraic circuit is a directed acyclic graph with the sources labeled by a variable name from the set $x_1, \ldots, x_n$, and each non-source node has in-degree two and is labeled by an operator from the set \{+,-,\times\}. There is a single sink in the graph, i.e., the output node.

Definition
\[
\text{ZEROP} = \{ C \mid \text{C an algebraic circuit that always outputs zero} \}.
\]
1. Choose $n$ random numbers $x_1,\ldots,x_n$ from 1 to $10 \cdot 2^m$.
2. Choose a random number $k \in [2^{2^m}]$ uniformly at random.
3. Evaluate the circuit $C$ on $x_1,\ldots,x_n$ modulo $k$ to obtain an output $y \mod k$ where $y = C(x_1,\ldots,x_n)$.
4. Accept if $y \mod k = 0$, and reject otherwise.
Let $G = (V, E)$ be a graph. A cut of $G$ is a partition $(S, T)$ of the vertex set $V$, i.e., $V = S \cup T$. Then we set

$$E(S, T) := \{ \{u, v\} \in E \mid u \in A, v \in B\},$$

and $\text{size}(S, T) := |E(S, T)|$.

We consider the Max Cut problem:

*Input:* A graph $G$.

*Output:* A cut $(S, T)$ with maximum size$(S, T)$.

**Theorem**

The Max Cut problem is NP-hard.
1. For every vertex $v$ in $G$ flip a fair coin.

2. If it is a head, then we put $v$ in to $S$ else to $T$.

**Theorem**

*The expected size of the cut produced by the algorithm is $|E|/2$.*

In fact, we only need *pairwise independence* in the proof.
Let $x_1, \ldots, x_n$ be random variables such that $x_i \in T$ for all $i \in [n]$ and $|T| = t$.

**Definition**

1. $x_i$’s are **independent** if for all $b_1, \ldots, b_n \in T$

   $$\Pr [x_1 = b_1 \land \ldots \land x_n = b_n] = \frac{1}{t^n}.$$  

2. $x_i$’s are **pairwise independent** if for all $i_1, i_2 \in [n]$ with $i_1 \neq i_2$ and $b_1, b_2 \in T$

   $$\Pr [x_{i_1} = b_1 \land x_{i_2} = b_2] = \frac{1}{t^2}.$$  

3. Let $k \in [n]$. Then $x_i$’s are **$k$-wise independent** if for all pairwise distinct $i_1, \ldots, i_k \in [n]$ and $b_1, \ldots, b_k \in T$

   $$\Pr [x_{i_1} = b_1 \land \ldots \land x_{i_k} = b_k] = \frac{1}{t^k}.$$
Examples

<table>
<thead>
<tr>
<th>$r_1$</th>
<th>$r_2$</th>
<th>$r_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

completely independent

<table>
<thead>
<tr>
<th>$r_1$</th>
<th>$r_2$</th>
<th>$r_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

pairwise independent

$r_3 := r_1 \oplus r_2$
Generating pairwise independent bits

Let $x_1, \ldots, x_k$ be $k$ completely random 0-1 variables. For every nonempty $S \subseteq [k]$ we let

$$X_S := \bigoplus_{i \in S} x_i.$$

**Theorem**

The $2^k - 1$ variables $X_S$’s are pairwise independent.
Let $q$ be a prime number. We want to generate $q$ pairwise independent numbers in $\mathbb{Z}_q = \{0, 1, \ldots, q - 1\}$.

1. Choose $a, b \in \mathbb{Z}_q$ independently and uniformly at random.
2. For every $i \in \mathbb{Z}_q$ output $r_i := a \cdot i + b \mod q$.

Lemma

$r_0, \ldots, r_{q-1}$ are pairwise independent.
The Constant-Depth Complexity of $k$-Clique
Let $S$ be a set and $s \in \mathbb{N}$. We use the notation 

$$\binom{S}{s} := \{ A \mid A \subseteq S \text{ with } |A| = s \}.$$ 

Thus $|\binom{S}{s}| = \binom{|S|}{s}$. Moreover, for every ordered $S$, we fix a reasonable bijection 

$$e_{s,S} : \left[ \binom{|S|}{s} \right] \to \binom{S}{s}.$$
Let $n \in \mathbb{N}$ and $G$ a graph with $V(G) = [n]$. Then $E(G) \subseteq \binom{[n]}{2}$. And $G$ can be identified with a binary string of length $\ell := \binom{n}{2}$

$$b(G) := b_1, \ldots, b_\ell \in \{0, 1\}^{\binom{n}{2}}$$

such that for every $i \in [\ell]$

$$b_i = \begin{cases} 
1 & \text{if } e_{[n],2}(i) \in E(G), \\
0 & \text{otherwise}.
\end{cases}$$

We use $G_n$ to denote (the encoding of) all graphs $G$ with $V(G) = [n]$, or formally

$$G_n = \{0, 1\}^{\binom{n}{2}}.$$
The $k$-clique problem

Let $k \in \mathbb{N}$ be a fixed constant.

$k$-CLIQUE

\begin{itemize}
  \item **Input:** A graph $G$.
  \item **Problem:** Decide whether there is a $K \in \binom{V(G)}{k}$ such that
    \begin{align*}
    \{u, v\} &\in E(G) \text{ for every distinct } u, v \in K.
    \end{align*}
\end{itemize}

$k$-CLIQUE can be understood as a sequence of functions

\[
\left( f_n^k \right)_{n \in \mathbb{N}}
\]

such that $f_n^k : \left\{0, 1\right\}^{\binom{n}{2}} \rightarrow \{0, 1\}$ for every $n \in \mathbb{N}$ and such that for every graph $G$ with $V(G) = [n]$

\[
f_n^k \left( b(G) \right) = 1 \iff G \text{ contains a } k\text{-clique}.
\]
A trivial upper bound

$k$-CLIQUE can be computed by the following sequence of circuits (formulas)

\[ f_n^k = \bigvee_{\mathcal{K} \in \binom{[n]}{k}} \bigwedge_{\{i,j\} \in \binom{\mathcal{K}}{2}} x_{\{i,j\}} , \]

which are of size \( n^{k+O(1)} \).

Observe that the above circuits are of constant depth.
We fix a constant $d \in \mathbb{N}$ and for every $n \in \mathbb{N}$ define

$$\theta_d(n) := \{\text{size}(C) \mid C \text{ a circuit of depth } d \text{ which computes } f_n^k\}.$$ 

Theorem (Rossman, 2008)

$$\theta_d(n) = \omega(n^{k/4}).$$
Let $f$ be a function whose domain is $G_n$. Consider a graph $G \in G_n$ and $A \subseteq [n]$. Let

$$
T^f,G(A) := \{ a \mid \text{there is a } B \subseteq A \text{ with } f(G \cup K_B) \neq f(G \cup K_B \setminus \{a\}) \}.
$$

$A$ is fully clique-sensitive under $f$, if $T^f,G(A) = A$.

For every $s \in \mathbb{N}$ we set

$$
T^f,G_s(A) := \bigcup_{B \subseteq A, |B| \leq s} T^f,G(B).
$$

Clearly

$$
T^f,G_1(A) = \emptyset.
$$
Lemma

(i) \( T_s^f, G (A) \subseteq T^f, G (A) \subseteq A \).

(ii) If \( A \subseteq B \), then \( T^f, G (A) \subseteq T^f, G (B) \) and \( T_s^f, G (A) \subseteq T_s^f, G (B) \).

(iii) If \( f : G_n \to \{0, 1\}^m \) where \( f_1, \ldots, f_m : G_n \to \{0, 1\} \) are individual coordinate-functions of \( f \), then

\[
T^f, G (A) = \bigcup_{i \in [m]} T^f_{i_1}, G (A) \quad \text{and} \quad T_s^f, G (A) = \bigcup_{i \in [m]} T_s^{f_i}, G (A).
\]

(iv) If \( A \) and \( B \) are fully clique-sensitive under \( f \), then so is \( A \cup B \).
Lemma
Let \( T := T^f_s, G(A) \). Then for every \( T \subseteq B \subseteq A \) with \( |B| \leq s \) we have
\[
f(G \cup K_T) = f(G \cup K_B).
\]

Proof.
Let \( b_1, \ldots, b_m \) enumerate the set \( B \setminus T \). For every \( i \in [m] \) we have
\[
f\left( G \cup K_{T \cup \{b_1, \ldots, b_i\}} \right) = f\left( G \cup K_{T \cup \{b_1, \ldots, b_i-1\}} \right),
\]
otherwise \( b_i \in T^f_s, G(B) \subseteq T^f_s, G(A) = T \). \( \square \)
Lemma

\[ T^f_G(A) = \bigcup \{ B \subseteq A \mid T^f_G(B) = B \text{ and } |B| \leq s \} \].

Proof.
\( \supseteq \) is trivial. Now consider an \( a \in T^f_G(A) \). So we have a \( B \subseteq A \) with

\[ f(G \cup K_B) \neq f(G \cup K_B \{a\}) \].

Choose such a \( B \) with minimum size, and we claim \( B \) is fully clique-sensitive. Assume there is \( b \in B \setminus T^f_G(B) \), thus

\[ f(G \cup K_B) = f(G \cup K_B \{b\}) \quad \text{and} \quad f(G \cup K_B \{a\}) = f(G \cup K_B \{a, b\}) \].

By the minimality of \( B \) (with respect to \( a \)) we conclude

\[ f(G \cup K_B) = f(G \cup K_B \{b\}) = f(G \cup K_B \{a, b\}) = f(G \cup K_B \{a\}) \]. \( \square \)
Lemma

1. $\mathbb{T}_{s}^{f,G}(A) \neq \emptyset$ if and only if $A$ has a fully clique-sensitive subset $B$ with $2 \leq |B| \leq s$.

2. $|\mathbb{T}_{s}^{f,G}(A)| > s$ if and only if $A$ has two fully clique-sensitive subsets $B$ and $C$ with $|B| \leq s$, $|C| \leq s$, and $|B \cup C| \geq s + 1$.

3. $|\mathbb{T}_{s}^{f,G}(A)| > s$ if and only if $A$ has a fully clique-sensitive subset $D$ with $s + 1 \leq |D| \leq 2 \cdot s$. 
The implications from right to left are all trivial.

1. By the previous lemma, $\mathbb{T}_s^f, G(A)$ is the union of all clique-sensitive subsets of $A$ of size at most $s$:
   \[ B_1, \ldots, B_m. \]
   Clearly $2 \leq |B_i| \leq s$ for all $i \in [m]$.

2. Let $i \in [m - 1]$ be the maximum index with
   \[ \left| \bigcup_{j \in [i]} B_j \right| \leq s. \]
   Then we can take the desired $B := \bigcup_{j \in [i]} B_j$ and $C := B_{i+1}$.

3. Let $D := B \cup C$. \qed
Let $C$ be a single-output circuit with $\binom{n}{2}$ inputs. For every node $\nu$ in $C$

(i) $C_\nu$ – the subcircuit of $C$ with single output $\nu$,

(ii) $C^\bullet_\mu$ – the same subcircuit but with outputs including $\nu$ and all its children.
Lemma

Let $G \in G_n$, $A \subseteq [n]$, and $s \geq 2$. If

$$T_s^{C,G}(A) = \emptyset \quad \text{and} \quad |T_s^{C\cup A,G}(A)| \leq s$$

for all nodes $\nu$ in $C$, then

$$C(G) = C(G \cup K_A).$$
Proof (1)

For every node $\nu$ in $C$ we let

$$T(\nu) := T^C_s \cdot G(A) \quad \text{and} \quad T^\bullet(\nu) := T^C_s \cdot G(A).$$

We note

$$T^\bullet(\nu) = T(\nu) \cup \bigcup_{\text{children } \mu \text{ of } \nu} T(\mu),$$

and

$$|T^\bullet(\nu)| \leq s.$$
We first prove for all nodes $\nu$ in $C$ by induction on the depth of $\nu$ that

$$C_{\nu}(G \cup K_{T^\bullet(\nu)}) = C_{\nu}(G \cup K_A).$$

Let $\nu$ be an input node corresponding to some $e \in (\binom{n}{2})$.

- If $e \subseteq A$, then
  $$T^\bullet(\nu) = T(\nu) = \mathbb{T}_s^{C_{\nu},G}(A) = \begin{cases} \emptyset & \text{if } e \in E(G), \\ e & \text{otherwise.} \end{cases}$$
  Hence, always $C_{\nu}(G \cup K_{T^\bullet(\nu)}) = C_{\nu}(G \cup K_A) = 1$.

- If $e \not\subseteq A$, then
  $$T^\bullet(\nu) = T(\nu) = \mathbb{T}_s^{C_{\nu},G}(A) = \emptyset.$$
  Then, $C_{\nu}(G \cup K_{T^\bullet(\nu)}) = C_{\nu}(G \cup K_A) = 1$ if $e \in E(G)$, and $0$ otherwise.
Let $\nu$ be a node with depth at least 2 and $\mu$ one of its children. Recall $T(\mu) \subseteq T^\bullet(\mu) \subseteq A$ and $|T^\bullet(\mu)| \leq s$, thus

$$C_\mu(G \cup K_{T(\mu)}) = C_\mu(G \cup K_{T^\bullet(\mu)}).$$

Similarly, as $T(\mu) \subseteq T^\bullet(\nu) \subseteq A$ and $|T^\bullet(\nu)| \leq s$,

$$C_\mu(G \cup K_{T(\mu)}) = C_\mu(G \cup K_{T^\bullet(\nu)}).$$

Therefore,

$$C_\mu(G \cup K_{T^\bullet(\nu)}) = C_\mu(G \cup K_{T^\bullet(\mu)}) = C_\mu(G \cup K_A)$$

by induction hypothesis.

Since $\mu$ is an arbitrary child of $\nu$, we conclude

$$C_\nu(G \cup K_{T^\bullet(\nu)}) = C_\nu(G \cup K_A).$$
Proof (4)

Let $\mu_{\text{out}}$ be the output node of $C$, thus $C_{\mu_{\text{out}}} = C$. It follows that

$$C(G \cup K_{T \bullet(\mu_{\text{out}})}) = C_{\mu_{\text{out}}} (G \cup K_{T \bullet(\mu_{\text{out}})}) = C_{\mu_{\text{out}}} (G \cup K_A) = C(G \cup K_A).$$

Again by $T(\mu_{\text{out}}) \subseteq T^\bullet(\mu_{\text{out}}) \subseteq A$ and $|T^\bullet(\mu_{\text{out}})| \leq s$ we have

$$C_{\mu_{\text{out}}} (G \cup K_{T(\mu_{\text{out}})}) = C_{\mu_{\text{out}}} (G \cup K_{T \bullet(\mu_{\text{out}})}),$$

that is,

$$C(G \cup K_{T(\mu_{\text{out}})}) = C(G \cup K_{T \bullet(\mu_{\text{out}})}).$$

Recall

$$T(\mu_{\text{out}}) = T_{s,C,G}^A = \emptyset.$$

Putting all the pieces together

$$C(G) = C(G \cup K_{T(\mu_{\text{out}})}) = C(G \cup K_A).$$
Definition
Let $n \in \mathbb{N}$ and $p \in \mathbb{R}$ with $0 \leq p \leq 1$. Then $G \in \text{ER}(n, p)$ is the Erdős-Rényi random graph on vertex set $[n]$ constructed by adding every edge $e \in \binom{[n]}{2}$ independently with probability $p$. 
Let $k \in \mathbb{N}$. Then the expected number of $k$-cliques in $G \in \text{ER}(n, p)$ is

$$E_k = \binom{n}{k} \cdot p^k.$$

Thus, if

$$p \ll n^{-2/(k-1)},$$

then with high probability, $G$ contains no $k$-clique.