# Model Counting meets Distinct Elements 

Kuldeep S. Meel<br>School of Computing<br>National University of Singapore<br>Joint work with Arnab Bhattacharyya, A. Pavan, and N.V. Vinodchandran

## Model Counting

- Given
- Boolean variables $X_{1}, X_{2}, \cdots X_{n}$
- Formula $\varphi$ over $X_{1}, X_{2}, \cdots X_{n}$
- $\operatorname{Sol}(\varphi)=\{$ satisfying assignments (aka models) of $\varphi$ \}


## Model Counting

- Given
- Boolean variables $X_{1}, X_{2}, \cdots X_{n}$
- Formula $\varphi$ over $X_{1}, X_{2}, \cdots X_{n}$
- $\operatorname{Sol}(\varphi)=\{$ satisfying assignments (aka models) of $\varphi$ \}
- Model Counting: Determine $|\operatorname{Sol}(\varphi)|$


## Model Counting

- Given
- Boolean variables $X_{1}, X_{2}, \cdots X_{n}$
- Formula $\varphi$ over $X_{1}, X_{2}, \cdots X_{n}$
- $\operatorname{Sol}(\varphi)=\{$ satisfying assignments (aka models) of $\varphi$ \}
- Model Counting: Determine $|\operatorname{Sol}(\varphi)|$
- Example $\varphi:=\left(X_{1} \vee X_{2}\right)$


## Model Counting

- Given
- Boolean variables $X_{1}, X_{2}, \cdots X_{n}$
- Formula $\varphi$ over $X_{1}, X_{2}, \cdots X_{n}$
- $\operatorname{Sol}(\varphi)=\{$ satisfying assignments (aka models) of $\varphi$ \}
- Model Counting: Determine $|\operatorname{Sol}(\varphi)|$
- Example $\varphi:=\left(X_{1} \vee X_{2}\right)$
- $\operatorname{Sol}(\varphi)=\{(0,1),(1,0),(1,1)\}$


## Model Counting

- Given
- Boolean variables $X_{1}, X_{2}, \cdots X_{n}$
- Formula $\varphi$ over $X_{1}, X_{2}, \cdots X_{n}$
- $\operatorname{Sol}(\varphi)=\{$ satisfying assignments (aka models) of $\varphi$ \}
- Model Counting: Determine $|\operatorname{Sol}(\varphi)|$
- Example $\varphi:=\left(X_{1} \vee X_{2}\right)$
- $\operatorname{Sol}(\varphi)=\{(0,1),(1,0),(1,1)\}$
- $|\operatorname{Sol}(\varphi)|=3$


## Model Counting

- Given
- Boolean variables $X_{1}, X_{2}, \cdots X_{n}$
- Formula $\varphi$ over $X_{1}, X_{2}, \cdots X_{n}$
- $\operatorname{Sol}(\varphi)=\{$ satisfying assignments (aka models) of $\varphi$ \}
- Model Counting: Determine $|\operatorname{Sol}(\varphi)|$
- Example $\varphi:=\left(X_{1} \vee X_{2}\right)$
- $\operatorname{Sol}(\varphi)=\{(0,1),(1,0),(1,1)\}$
- $|\operatorname{Sol}(\varphi)|=3$

Problem Compute $(\varepsilon, \delta)$ approximation of $|\operatorname{Sol}(\varphi)|$
Concern Number of NP Queries

## Applications across Computer Science



## Distinct Elements

- Given a stream $\mathbf{a}=a_{1}, a_{2}, \ldots a_{m}$ where $a_{i} \in\{0,1\}^{n}$
- $\operatorname{DE}(\mathbf{a})=\left|\cup_{i} a_{i}\right|$
- Also known as $F_{0}$ estimation


## Distinct Elements

- Given a stream $\mathbf{a}=a_{1}, a_{2}, \ldots a_{m}$ where $a_{i} \in\{0,1\}^{n}$
- $\operatorname{DE}(\mathbf{a})=\left|\cup_{i} a_{i}\right|$
- Also known as $F_{0}$ estimation
- Example $\mathbf{a}=1,2,1,1,2,1,3,5,1,2,1,3$
- $\mathrm{F}_{0}(\mathbf{a})=\left|\cup_{i} a_{i}\right|=|\{1,2,3,5\}|=4$


## Distinct Elements

- Given a stream $\mathbf{a}=a_{1}, a_{2}, \ldots a_{m}$ where $a_{i} \in\{0,1\}^{n}$
- $\operatorname{DE}(\mathbf{a})=\left|\cup_{i} a_{i}\right|$
- Also known as $F_{0}$ estimation
- Example $\mathbf{a}=1,2,1,1,2,1,3,5,1,2,1,3$
- $\mathrm{F}_{0}(\mathbf{a})=\left|\cup_{i} a_{i}\right|=|\{1,2,3,5\}|=4$
- Fundamental problem in databases with a long history of work


## Distinct Elements

- Given a stream $\mathbf{a}=a_{1}, a_{2}, \ldots a_{m}$ where $a_{i} \in\{0,1\}^{n}$
- $\operatorname{DE}(\mathbf{a})=\left|\cup_{i} a_{i}\right|$
- Also known as $F_{0}$ estimation
- Example $\mathbf{a}=1,2,1,1,2,1,3,5,1,2,1,3$
- $\mathrm{F}_{0}(\mathbf{a})=\left|\cup_{i} a_{i}\right|=|\{1,2,3,5\}|=4$
- Fundamental problem in databases with a long history of work Problem Compute $(\varepsilon, \delta)$ approximation of $F_{0}$ Concern Space Complexity


## Hashing-Based Techniques

Model Counting
(S83,GSS06,GHSS07,CMV13b,EGSS13b,CMV14,CDR15,CMV16,ZCSE16,AD16 KM18,ATD18,SM19,ABM20,SGM20)

Distinct Elements
(FM85,AMS99,GT01,BKS02,BJKST02, CM03,CLKB04,PT07, TW12,SP09)

## 2-wise independent Hashing

- Let $H$ be family of 2 -wise independent hash functions mapping $\{0,1\}^{n}$ to $\{0,1\}^{m}$

$$
\begin{gathered}
\forall y_{1}, y_{2} \in\{0,1\}^{n}, \alpha_{1}, \alpha_{2} \in\{0,1\}^{m}, h \stackrel{R}{\leftarrow} H \\
\operatorname{Pr}\left[h\left(y_{1}\right)=\alpha_{1}\right]=\operatorname{Pr}\left[h\left(y_{2}\right)=\alpha_{2}\right]=\left(\frac{1}{2^{m}}\right) \\
\operatorname{Pr}\left[h\left(y_{1}\right)=\alpha_{1} \wedge h\left(y_{2}\right)=\alpha_{2}\right]=\left(\frac{1}{2^{m}}\right)^{2}
\end{gathered}
$$

## 2-wise independent Hash Functions

- Variables: $X_{1}, X_{2}, \cdots X_{n}$
- To construct $h:\{0,1\}^{n} \rightarrow\{0,1\}^{m}$, choose $m$ random XORs
- Pick every $X_{i}$ with prob. $\frac{1}{2}$ and XOR them
- $X_{1} \oplus X_{3} \oplus X_{6} \cdots \oplus X_{n-2}$
- Expected size of each XOR: $\frac{n}{2}$


## 2-wise independent Hash Functions

- Variables: $X_{1}, X_{2}, \cdots X_{n}$
- To construct $h:\{0,1\}^{n} \rightarrow\{0,1\}^{m}$, choose $m$ random XORs
- Pick every $X_{i}$ with prob. $\frac{1}{2}$ and XOR them
- $X_{1} \oplus X_{3} \oplus X_{6} \cdots \oplus X_{n-2}$
- Expected size of each XOR: $\frac{n}{2}$
- To choose $\alpha \in\{0,1\}^{m}$, set every XOR equation to 0 or 1 randomly

$$
\begin{align*}
x_{1} \oplus x_{3} \oplus x_{6} \cdots \oplus x_{n-2} & =0  \tag{1}\\
x_{2} \oplus x_{5} \oplus x_{6} \cdots \oplus x_{n-1} & =1  \tag{2}\\
& \cdots \\
x_{1} \oplus x_{2} \oplus x_{5} \cdots \oplus x_{n-2} & =1
\end{align*}
$$

- Therefore, $h(X)=\alpha$ can be represented as $A X=b$

As Simple as Counting Dots


As Simple as Counting Dots


## As Simple as Counting Dots

Pick a random cell


Estimate $=$ Number of models in a cell $\times$ Number of cells

## Challenges

Challenge 1 How to partition into roughly equal small cells of solutions without knowing the distribution of solutions?

## Challenges

Challenge 1 How to partition into roughly equal small cells of solutions without knowing the distribution of solutions?

Challenge 2 How many cells?

## Challenges

Challenge 1 How to partition into roughly equal small cells of solutions without knowing the distribution of solutions?
2-wise independent hash functions

## ApproxMC



## ApproxMC



## ApproxMC



## ApproxMC



## ApproxMC



## Distinct Elements

```
Choose \(h:\{0,1\}^{n} \mapsto\{0,1\}^{n}\)
minhash \(\leftarrow 2^{n}\);
for \(a_{i} \in\) a do
    if \(h\left(a_{i}\right)<\) minhash then
            minhash \(=h\left(a_{i}\right)\)
    end if
end for
return \(\frac{2^{n}}{\text { minhash }}\)
```


## Is there more than meets the eyes?

- From Distinct Elements to Counting
- From Counting to Distinct Elements


## Hashing-based Distinct Elements

1: $h \leftarrow$ ChooseHashFunctions
2: $\mathcal{S} \leftarrow\}$
3: for $a_{i} \in \mathbf{a}$ do
ProcessUpdate(S, $\left.h, a_{i}\right)$
end for
6: Est $\leftarrow$ ComputeEst(S)
7: Return Est

## Hashing-based Distinct Elements

1: $h \leftarrow$ ChooseHashFunctions
2: $\mathcal{S} \leftarrow\}$
3: for $a_{i} \in$ a do
ProcessUpdate(S, $\left.h, a_{i}\right)$
end for
6: Est $\leftarrow$ ComputeEst( $\mathcal{S}$ )
7: Return Est
Different Algorithms based on ProcessUpdate

- Minimum: Keep track of minimum $h\left(a_{i}\right)$
- Bucketing


## Hashing-based Distinct Elements

1: $h \leftarrow$ ChooseHashFunctions
2: $\mathcal{S} \leftarrow\}$
3: for $a_{i} \in$ a do
ProcessUpdate(S, $\left.h, a_{i}\right)$
end for
6: Est $\leftarrow$ ComputeEst( $\mathcal{S}$ )
7: Return Est
Different Algorithms based on ProcessUpdate

- Minimum: Keep track of minimum $h\left(a_{i}\right)$
- Bucketing
- ...


## From Distinct Elements to Counting: A Two Step Recipe

$\mathbf{a}_{u}$ : set of all distinct elements of the stream $\mathbf{a}$.

Key Idea The formula $\varphi$ can viewed as symbolic representation of some set $\mathbf{a}_{u}$ such that $\operatorname{Sol}(\varphi)=\mathbf{a}_{u}$.

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, h , and the set $\mathbf{a}_{u}$ at the end of stream.

Step 2 Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds. And now, we can estimate $|\operatorname{Sol}(\varphi)|$ from $\mathcal{S}$.

## Min-based Estimation

```
Choose \(h:\{0,1\}^{n} \mapsto\{0,1\}^{n}\)
minhash \(\leftarrow 2^{n}\);
for \(a_{i} \in \mathbf{a}\) do
    if minhash \(<h\left(a_{i}\right)\) then
            minhash \(=h\left(a_{i}\right)\)
    end if
end for
return \(\frac{2^{n}}{\text { minhash }}\)
```


## Application I: Min-based Counting Algorithm

Step1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, h , and the set $\mathbf{a}_{u}$ at the end of stream.

## Application I: Min-based Counting Algorithm

Step1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, h , and the set $\mathbf{a}_{u}$ at the end of stream.
$\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}:=\min _{y \in a_{u}} h(y)$

## Application I: Min-based Counting Algorithm

Step1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, h , and the set $\mathbf{a}_{u}$ at the end of stream.

$$
\begin{aligned}
& \mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}:=\min _{y \in a_{u}} h(y) \\
& \mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi)) \mathcal{S}:=\min _{y \in \operatorname{Sol}(\varphi)} h(y)
\end{aligned}
$$

## Application I: Min-based Counting Algorithm

Step1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, h , and the set $\mathbf{a}_{u}$ at the end of stream.

$$
\begin{aligned}
& \mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}:=\min _{y \in a_{u}} h(y) \\
& \mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi)) \mathcal{S}:=\min _{y \in \operatorname{Sol}(\varphi)} h(y)
\end{aligned}
$$

Step2 Given a formula $\varphi$ and set of hash functions $H$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds. And now, we can estimate $|\operatorname{Sol}(\varphi)|$ from $\mathcal{S}$.

- Use polynomially many calls to NP Oracle to determine $\mathcal{S}$


## Bucketing-based Streaming Algorithm

```
Choose \(h:\{0,1\}^{n} \mapsto\{0,1\}^{n}\)
\(\ell \leftarrow 0 ; \mathcal{B} \leftarrow \emptyset\)
for \(a_{i} \in\) a do
        if \(h\left(a_{i}\right) \bmod 2^{\ell}=0^{\ell}\) then
            \(\mathcal{B}\).Append \(\left(a_{i}\right)\)
            if \(|\mathcal{B}| \geq\) thresh then
                \(\ell++\)
            Filter \((\mathcal{B}, h, \ell)\)
        end if
    end if
end for
return \(|\mathcal{B}| \times 2^{\ell}\)
```


## Bucketing-based Streaming Algorithm

```
Choose \(h:\{0,1\}^{n} \mapsto\{0,1\}^{n}\)
\(\ell \leftarrow 0 ; \mathcal{B} \leftarrow \emptyset\)
for \(a_{i} \in\) a do
    if \(h\left(a_{i}\right) \bmod 2^{\ell}=0^{\ell}\) then
    \(\mathcal{B} . \operatorname{Append}\left(a_{i}\right)\)
            if \(|\mathcal{B}| \geq\) thresh then
                \(\ell++\)
                Filter \((\mathcal{B}, h, \ell)\)
            end if
        end if
end for
return \(|\mathcal{B}| \times 2^{\ell}\)
```

Elements that satisfy XOR

Add another XOR

## Application II: Bucketing-based Counting Algorithm

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, hash function $h$ and set $\mathbf{a}_{u}$ at the end of stream.

## Application II: Bucketing-based Counting Algorithm

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, hash function $h$ and set $\mathbf{a}_{\mu}$ at the end of stream.

$$
\begin{gathered}
\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
\left|\left\{\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh. }
\end{gathered}
$$

## Application II: Bucketing-based Counting Algorithm

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, hash function $h$ and set $\mathbf{a}_{u}$ at the end of stream.

$$
\begin{aligned}
& \mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \quad\left|\left\{\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh. } \\
& \mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi)): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \left|\left\{\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh }
\end{aligned}
$$

## Application II: Bucketing-based Counting Algorithm

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, hash function $h$ and set $\mathbf{a}_{\mu}$ at the end of stream.

$$
\begin{aligned}
& \mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \quad\left|\left\{\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh. } \\
& \mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi)): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \left|\left\{\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh }
\end{aligned}
$$

Step 2 Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds. And now, we can estimate $|\operatorname{Sol}(\varphi)|$ from $\mathcal{S}$.

## Application II: Bucketing-based Counting Algorithm

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, hash function $h$ and set $\mathbf{a}_{u}$ at the end of stream.

$$
\begin{aligned}
& \mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \quad\left|\left\{\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh. } \\
& \mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi)): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \left|\left\{\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh }
\end{aligned}
$$

Step 2 Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds. And now, we can estimate $|\operatorname{Sol}(\varphi)|$ from $\mathcal{S}$.

- Use polynomially many calls to NP Oracle to determine $\mathcal{S}$


## Application II: Bucketing-based Counting Algorithm

Step 1 Capture the relationship $\mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right)$ between the sketch $\mathcal{S}$, hash function $h$ and set $\mathbf{a}_{\mu}$ at the end of stream.

$$
\begin{aligned}
& \mathcal{P}\left(\mathcal{S}, h, \mathbf{a}_{u}\right): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \quad\left|\left\{\mathbf{a}_{u} \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh. } \\
& \mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi)): \mathcal{S}=(\ell, \mathcal{B}) \text { such that } \mathcal{B}=\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell}\right) \text { and } \\
& \left|\left\{\operatorname{Sol}(\varphi) \cap h^{-1}\left(0^{\ell-1}\right)\right\}\right|>\text { thresh and }|\mathcal{B}| \leq \text { thresh }
\end{aligned}
$$

Step 2 Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds. And now, we can estimate $|\operatorname{Sol}(\varphi)|$ from $\mathcal{S}$.

- Use polynomially many calls to NP Oracle to determine $\mathcal{S}$

This is ApproxMC!

## From Distinct Elements to Counting: Implications

Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds.

## Theorem (FPRAS)

If construction of sketch $\mathcal{S}$ is in PTIME for a class of formulas, then there is FPRAS for the corresponding class. E.g.: DNF, Union of XORs

## From Distinct Elements to Counting: Implications

Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds.

## Theorem (FPRAS)

If construction of sketch $\mathcal{S}$ is in PTIME for a class of formulas, then there is FPRAS for the corresponding class. E.g.: DNF, Union of XORs

[^0]
## From Distinct Elements to Counting: Implications

Given a formula $\varphi$ and hash function $h$, design an algorithm to construct sketch $\mathcal{S}$ such that $\mathcal{P}(\mathcal{S}, h, \operatorname{Sol}(\varphi))$ holds.

## Theorem (FPRAS)

If construction of sketch $\mathcal{S}$ is in PTIME for a class of formulas, then there is FPRAS for the corresponding class. E.g.: DNF, Union of XORs

## Theorem (Space and Query)

$p(n)$ space algorithms in streaming imply $(p(n))^{2}$ NP query complexity algorithms for model counting

Theorem (Lower Bounds)
Lower bounds for Distributed Streaming translate to lower bounds for Distributed DNF counting

Is there more to it than meets the eyes?

- From Distinct Elements to Counting
- From Counting to Distinct Elements


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas
- A stream can be viewed as a DNF
- $a=a_{1}, a_{2}, a_{3}, \ldots a_{m}$


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas
- A stream can be viewed as a DNF
- $a=a_{1}, a_{2}, a_{3}, \ldots a_{m}$
- $\left|\cup_{i} a_{i}\right|=\left|\operatorname{Sol}\left(a_{1} \vee a_{2} \vee a_{3} \vee a_{m}\right)\right|$
- $a_{i}$ is represented by conjunction of $n$ literals $X_{1}, X_{2}, \ldots X_{n}$.


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas
- A stream can be viewed as a DNF
- $a=a_{1}, a_{2}, a_{3}, \ldots a_{m}$
- $\left|\cup_{i} a_{i}\right|=\left|\operatorname{Sol}\left(a_{1} \vee a_{2} \vee a_{3} \vee a_{m}\right)\right|$
- $a_{i}$ is represented by conjunction of $n$ literals $X_{1}, X_{2}, \ldots X_{n}$.
- So hashing-based FPRAS for DNF $\Longrightarrow F_{0}$ estimation


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas
- A stream can be viewed as a DNF
- $a=a_{1}, a_{2}, a_{3}, \ldots a_{m}$
- $\left|\cup_{i} a_{i}\right|=\left|\operatorname{Sol}\left(a_{1} \vee a_{2} \vee a_{3} \vee a_{m}\right)\right|$
- $a_{i}$ is represented by conjunction of $n$ literals $X_{1}, X_{2}, \ldots X_{n}$.
- So hashing-based FPRAS for DNF $\Longrightarrow F_{0}$ estimation
- A general scheme for structured sets


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas
- A stream can be viewed as a DNF
- $a=a_{1}, a_{2}, a_{3}, \ldots a_{m}$
- $\left|\cup_{i} a_{i}\right|=\left|\operatorname{Sol}\left(a_{1} \vee a_{2} \vee a_{3} \vee a_{m}\right)\right|$
- $a_{i}$ is represented by conjunction of $n$ literals $X_{1}, X_{2}, \ldots X_{n}$.
- So hashing-based FPRAS for DNF $\Longrightarrow F_{0}$ estimation
- A general scheme for structured sets
- Encompasses models such as ranges, affine spaces


## From Counting to Distinct Elements

- ApproxMC is FPRAS for DNF formulas
- A stream can be viewed as a DNF
- $a=a_{1}, a_{2}, a_{3}, \ldots a_{m}$
- $\left|\cup_{i} a_{i}\right|=\left|\operatorname{Sol}\left(a_{1} \vee a_{2} \vee a_{3} \vee a_{m}\right)\right|$
- $a_{i}$ is represented by conjunction of $n$ literals $X_{1}, X_{2}, \ldots X_{n}$.
- So hashing-based FPRAS for DNF $\Longrightarrow F_{0}$ estimation
- A general scheme for structured sets
- Encompasses models such as ranges, affine spaces
- Application: Distinct Elements over Range
- Every item $\left[a_{i}, b_{i}\right]$ can be represented using a DNF formula.
- So just apply FPRAS for DNF


## Conclusion

Summary

- From Distinct Elements to Counting
- From Counting to Distinct Elements


## Conclusion

Summary

- From Distinct Elements to Counting
- From Counting to Distinct Elements

Future Directions

- Practical scalability of newly devised counting techniques
- Lifting Sparse Hashing techniques to streaming
- What is the analogue for higher moments ( $F_{k}$ )


[^0]:    Theorem (Space and Query)
    $p(n)$ space algorithms in streaming imply $(p(n))^{2}$ NP query complexity algorithms for model counting

