Model Counting

Tejas Anand

June 22, 2024

1 For Z_k

If our lets say our literals $x_1, x_2 \cdots x_q$ are from Z_k for $k > 2$ instead of $\{0, 1\}$, Then we would need to sample a hash function from $\mathcal{H}_k(n, m, r) =$ Set of hash functions from $Z_k^n \to Z_k^m$ which are r-wise independent. Note that $Z_k = \{0, 1, 2 \cdots k-1\}$ and $|Z_k^n| = k^n$.
Let's think about the exact hash family we would use for this later.

Let's think about what changes to the ApproxMCCore we would need to do First of all, the idea of the algorithm is to choose a random cell and check if it is non empty and has less than *pivot* elements. If yes, then we are all well and good, and we can take this count as a representative count for other cells as well. To get the total count we would just multiply this count by the number of cells. But if the cell has more than pivot elements, then we would try to decrease the number of elements in a given cell by making the number of cells larger. We do this by sampling a new hash function from the family $\mathcal{H}_k(n, m+1, r)$. This increases the number of cells by a factor of k, instead of 2 for boolean variables. We keep repeating this until we find a random cell having less than *pivot* elements or when the number of cells exceeds $\frac{k^{n+1}}{pivot}$.

The number of cells at any stage of the algorithm is k^{i-l}, so if we terminate when $i = n$, then the number of cells would be $\frac{k^n}{k^{\lfloor log_k pivot \rfloor - 1}} \geq \frac{k^{n+1}}{pivot}$

2 Analysis

Theorem 1. *Let Γ be the sum of of r-wise independent random variables, each of which is confined to the interval $[0, 1]$, and suppose that $E[\Gamma] = \mu$. For $0 < \beta \leq 1$, if $r \leq \lfloor \beta^2 \mu e^{-1/2} \rfloor \leq 4$, then $\Pr[|\Gamma - \mu| > \beta\mu] \leq e^{-r/2}$*

Lemma 1. *Let Algorithm* ApproxMCCore *when invoked from* ApproxMC *return a value c with the value of the loop counter being equal to i. Then $\Pr[(1+\varepsilon)^{-1}|R_F| \leq c \leq (1+\varepsilon)|R_F||c \neq \perp$ and $i \leq \log_k |R_F|] \geq 1 - e^{-3/2}$*

Algorithm 1 ApproxMCCore$(F, pivot)$

1: $S \leftarrow \mathsf{BoundedSMT}(F, pivot + 1)$ ▷ Assume $x_1, x_2 \cdots x_q$ are the variables of F
2: **if** $|S| \leq pivot$ **then**
3: **return** $|S|$;
4: **else**
5: $l \leftarrow \lfloor log_k(pivot) \rfloor - 1$; $i \leftarrow l - 1$
6: **repeat**
7: $i \leftarrow i + 1$;
8: Choose $h \leftarrow \mathcal{H}_k(n, i - l, 3)$ uniformly at random;
9: Choose $\alpha \leftarrow Z_k^{i-l}$ uniformly at random;
10: $S \leftarrow \mathsf{BoundedSMT}(F \wedge h(x_1, x_2 \cdots x_q) = \alpha, pivot + 1)$
11: **until** $(1 \leq |S| \leq pivot)$ or $(i = n)$;
12: **end if**
13: **if** $(|S| > pivot$ **or** $|S| = 0)$ **then**
14: **return** $\perp$;
15: **else**
16: **return** $|S| \cdot k^{i-l}$;
17: **end if**

Proof Other Information. The Lemma is trivially satisified when $|R_F| \leq pivot$. The expression of pivot is $pivot = k^2\lceil 3e^{1/2}(1 + \frac{1}{\varepsilon})^2\rceil$ Let's consider the case when $|R_F| > pivot$. The only case we need to consider is when the algorithm returns from line 17, with a value obtained from $k^{i-l} \cdot |R_{F,h,\alpha}|$. The value of i is always in $\{l \cdots n\}$. As $pivot < |R_F| \leq k^n$ and $l = \lfloor \log_k(pivot) \rfloor - 1$, We have $l < \log_k |R_F| \leq n$. The lemma is now proved by showing that for every i in $\{l \cdots \lfloor \log_k |R_F| \rfloor\}$, $h \in \mathcal{H}_k(n, i - l, 3)$, and $\alpha \in Z_k^{i-l}$, we have $\Pr[(1 + \varepsilon)^{-1}|R_F| \leq k^{i-l}|R_{F,h,\alpha}| \leq (1 + \varepsilon)|R_F|] \geq 1 - e^{-3/2}$. For every $y \in Z_k^n$ and for $\alpha \in Z_k^{i-l}$, We define an indicator random variable as follows $\gamma_{y,\alpha}(h) = 1$ if $h(y) = \alpha, 0$ otherwise . We fix y and α and choose h uniformly at random from $\mathcal{H}_k(n, i-l, 3)$. Thus $\Pr[\gamma_{y,\alpha} = 1] = \Pr[h(y) = \alpha] = k^{-(i-l)} = E[\gamma_{y,\alpha}]$. The 3-wise indpendence of the hash function implies that the random variables $\gamma_{y_a,\alpha}, \gamma_{y_b,\alpha}, \gamma_{y_c,\alpha}$ are independent for distinct values of y_a, y_b, y_c.

Let $\Gamma_\alpha = \sum_{y \in R_F} \gamma_{y,\alpha}$. Clearly Γ_α counts the satisfying models y with hash value equal to α. Hence $\Gamma_\alpha = |R_{F,h,\alpha}|$. $\mu_\alpha = E[\Gamma_\alpha] = k^{-(i-l)}|R_F|$. As $|R_F| > pivot$ and $i \leq \log_k |R_F|$ and $l = \lfloor \log_k(pivot) \rfloor - 1$, we have that $\log_k(pivot) - 2 < l \leq \log_k(pivot) - 1$ Thus $\log_k(\frac{pivot}{k^2}) < l \leq \log_k(\frac{pivot}{k})$. Which gives us $\frac{pivot}{k^2} < k^l$, Now using the expression of $pivot$, we get $\lceil 3e^{1/2}(1 + \frac{1}{\varepsilon})^2\rceil < k^l$, which gives us $3e^{1/2}(1 + \frac{1}{\varepsilon})^2 < k^l$. Also we must note that as $i \leq \log_k |R_F|$, we have $1 \leq \frac{|R_F|}{k^i}$. Thus, $3e^{1/2}(1 + \frac{1}{\varepsilon})^2 < k^l \leq \frac{|R_F|}{k^{i-l}}$, which gives us $3 \leq \lfloor e^{-1/2}(1 + \frac{1}{\varepsilon})^2 \frac{|R_F|}{k^{i-l}} \rfloor$. We can now use Theorem 1 to obtain $\Pr[(1 - \frac{\varepsilon}{1+\varepsilon})|R_F| \leq k^{i-l}|R_{F,h,\alpha}| \leq (1 + \frac{\varepsilon}{1+\varepsilon})|R_F|] \geq 1 - e^{-3/2}$. As $\varepsilon > \frac{\varepsilon}{1+\varepsilon}$ for $\varepsilon > 0$, We get $\Pr[(1 + \varepsilon)^{-1}|R_F| \leq k^{i-l}|R_{F,h,\alpha}| \leq (1 + \varepsilon)|R_F|] \geq \Pr[(1 - \frac{\varepsilon}{1+\varepsilon})|R_F| \leq k^{i-l}|R_{F,h,\alpha}| \leq (1 + \frac{\varepsilon}{1+\varepsilon})|R_F|] \geq 1 - e^{-3/2}$.

□