A. Appendix: Proofs

Lemma 3 (pairwise independent hash functions construction)**.** *Let $a \in \{0,1\}^n$, $b \in \{0,1\}$. Then the family $\mathcal{H} = \{h_{a,b}(x) : \{0,1\}^n \to \{0,1\}\}$ where $h_{a,b}(x) = a \cdot x + b \mod 2$ is a family of pairwise independent hash functions. The function $h_{a,b}(x)$ can be alternatively rewritten in terms of XORs operations $\oplus$, i.e. $h_{a,b}(x) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n \oplus b$.*

Proof. Uniformity is clear because it is the sum of uniform Bernoulli random variables over the field $\mathbb{F}(2)$ (arithmetic modulo 2). For pairwise independence, given any two configurations $x_1, x_2 \in \{0,1\}^n$, consider the sets of indexes $S_1 = \{i : x_1(i) = 1\}$, $S_2 = \{i : x_2(i) = 1\}$. Then

$$\begin{aligned} H(x_1) = & \sum_{i \in S_1 \cap S_2} a_i \oplus \sum_{i \in S_1 \setminus S_2} a_i \oplus b \\ = & \; R(S_1 \cap S_2) \oplus R(S_1 \setminus S_2) \oplus b \\ H(x_2) = & \; R(S_1 \cap S_2) \oplus R(S_2 \setminus S_1) \oplus b \end{aligned}$$

where $R(S) \triangleq \sum_{i \in S} a_i$. Note that $R(S_1 \cap S_2)$, $R(S_1 \setminus S_2)$, $R(S_2 \setminus S_1)$ and b are independent as they depend on disjoint subsets of independent variables. When $x_1 \neq x_2$, this implies that $(H(x_1), H(x_2))$ takes each value in $\{0,1\}^2$ with probability $1/4$. □

As pairwise independent random variables are fundamental tools for derandomization of algorithms, more complicated constructions based larger finite fields generated by a prime power $\mathbb{F}(q^k)$ where q is a prime number are known (Vadhan, 2011). These constructions require a smaller number of random bits as input, and would therefore reduce the variance of our algorithm (which is deterministic except for the randomized hash function use).

Proof of Proposition 1. Follows immediately from Lemma 3. □

Proof of Lemma 1. The cases where $i+c > n$ or $i-c < 0$ are obvious. For the other cases, let's define the set of the 2^j heaviest configurations as in Definition 2:

$$\mathcal{X}_j = \{\sigma_1, \sigma_2, \cdots, \sigma_{2^j}\}$$

Define the following random variable

$$S_j(h^i_{A,b}) \triangleq \sum_{\sigma \in \mathcal{X}_j} 1_{\{A\sigma = b \bmod 2\}}$$

which gives the number of elements of $\mathcal{X}_j$ satisfying i random parity constraints. The randomness is over the choice of A and b, which are uniformly sampled in $\{0,1\}^{i \times n}$ and $\{0,1\}^i$ respectively. By Proposition 1, $h^i_{A,b} : \Sigma \to \{0,1\}^i$ is sampled from a family of pairwise independent hash functions. Therefore, from the uniformity property in Definition 1, for any σ the random variable $1_{\{A\sigma = b \bmod 2\}}$ is Bernoulli with probability $1/2^i$. By linearity of expectation,

$$E[S_j(h^i_{A,b})] = \frac{|\mathcal{X}_j|}{2^i} = \frac{2^j}{2^i}$$

Further, from the pairwise independence property in Definition 1,

$$\begin{aligned} Var[S_j(h^i_{A,b})] &= \sum_{\sigma \in \mathcal{X}_j} Var\left[1_{\{A\sigma = b \bmod 2\}}\right] \\ &= \frac{2^j}{2^i}\left(1 - \frac{1}{2^i}\right) \end{aligned}$$

Applying Chebychev Inequality, we get that for any $k > 0$,

$$\Pr\left[\left|S_j(h^i_{A,b}) - \frac{2^j}{2^i}\right| > k\sqrt{\frac{2^j}{2^i}\left(1 - \frac{1}{2^i}\right)}\right] \leq \frac{1}{k^2}$$

Recall the definition of the random variable $w_i = \max_\sigma w(\sigma)$ subject to $A\sigma = b \mod 2$ (the randomness is over the choice of A and b). Then

$$\Pr[w_i \geq b_j] = \Pr[w_i \geq w(\sigma_{2^j})] \geq \Pr[S_j(h^i_{A,b}) \geq 1]$$

which is the probability that at least one configuration from $\mathcal{X}_j$ "survives" after adding i parity constraints.

To ensure that the probability bound $1/k^2$ provided by Chebychev Inequality is smaller than a $1/2$, we need $k > \sqrt{2}$. We use $k = 3/2$ for the rest of this proof, exploiting the following simple observations which hold for $k = 3/2$ and any $c \geq 2$:

$$\begin{aligned} k\sqrt{2^c} &\leq 2^c - 1 \\ k\sqrt{2^{-c}} &\leq 1 - 2^{-c} \end{aligned}$$

For $j = i + c$ and k and c as above, we have that

$$\begin{aligned} \Pr[w_i \geq b_{i+c}] \geq \Pr[S_{i+c}(h^i_{A,b}) \geq 1] \geq \\ \Pr\left[|S_{i+c}(h^i) - 2^c| \leq 2^c - 1\right] \geq \\ \Pr\left[|S_{i+c}(h^i) - 2^c| \leq k\sqrt{2^c}\right] \geq \\ \Pr\left[\left|S_{i+c}(h^i_{A,b}) - 2^c\right| \leq k\sqrt{2^c\left(1 - \frac{1}{2^i}\right)}\right] \geq \\ 1 - \frac{1}{k^2} = 5/9 > 1/2 \end{aligned}$$

Similarly, for $j = i - c$ and k and c as above, we have $\Pr[w_i \leq b_{i-c}] \geq 5/9 > 1/2$.

Finally, using Chernoff inequality (since $w_i^1, \cdots, w_i^T$ are i.i.d. realizations of w_i)

$$\Pr\left[M_i \leq b_{i-c}\right] \geq 1 - \exp(-\alpha'(c)T) \tag{5}$$
$$\Pr\left[M_i \geq b_{i+c}\right] \geq 1 - \exp(-\alpha'(c)T) \tag{6}$$

where $\alpha'(2) = 2(5/9 - 1/2)^2$, which gives the desired result

$$\begin{aligned}\Pr\left[b_{i+c} \leq M_i \leq b_{i-c}\right] &\geq 1 - 2\exp(\alpha'(c)T) \\ &= 1 - \exp(-\alpha^*(c)T)\end{aligned}$$

where $\alpha^*(2) = \ln 2\alpha'(2) = 2(5/9 - 1/2)^2 \ln 2 > 0.0042$ □

Proof of Lemma 2. Observe that we may rewrite L' as follows:

$$L' = b_0 + \sum_{i=n-c-1}^{n-1} b_n 2^i + \sum_{i=0}^{n-c-2} b_{i+c+1} 2^i = b_0 + \sum_{i=n-c-1}^{n-1} b_n 2^i + \sum_{j=c+1}^{n-1} b_j 2^{j-c-1}$$

Similarly,

$$U' = b_0 + \sum_{i=0}^{c-1} b_0 2^i + \sum_{i=c}^{n-1} b_{i+1-c} 2^i =$$
$$b_0 + \sum_{i=0}^{c-1} b_0 2^i + \sum_{j=1}^{n-c} b_j 2^{j+c-1} = 2^c b_0 + 2^c \sum_{j=1}^{n-c} b_j 2^{j-1} =$$
$$2^c b_0 + 2^c \left(\sum_{j=1}^{c} b_j 2^{j-1} + \sum_{j=c+1}^{n-c} b_j 2^{j-1} \right) \leq$$
$$2^c b_0 + 2^c \left(\sum_{j=1}^{c} b_0 2^{j-1} + \sum_{j=c+1}^{n-c} b_j 2^{j-1} \right) =$$
$$2^{2c} b_0 + 2^{2c} \sum_{j=c+1}^{n-c} b_j 2^{j-1-c} \leq$$
$$2^{2c} \left(b_0 + \sum_{i=n-c-1}^{n-1} b_n 2^i + \sum_{j=c+1}^{n-1} b_j 2^{j-c-1} \right) = 2^{2c} L'$$

This finishes the proof. □

Proof of Theorem 1. It is clear from the pseudocode of Algorithm 1 that it makes $\Theta(n \ln n \ln 1/\delta)$ MAP queries. For accuracy analysis, we can write W as:

$$W \triangleq \sum_{j=1}^{2^n} w(\sigma_j) = w(\sigma_1) + \sum_{i=0}^{n-1} \sum_{\sigma \in B_i} w(\sigma)$$
$$\in \left[b_0 + \sum_{i=0}^{n-1} b_{i+1} 2^i, b_0 + \sum_{i=0}^{n-1} b_i 2^i \right] \triangleq [L, U]$$

Note that $U \leq 2L$ because $2L = 2b_0 + \sum_{i=0}^{n-1} b_{i+1} 2^{i+1} = 2b_0 + \sum_{\ell=1}^{n} b_\ell 2^\ell = b_0 + \sum_{\ell=0}^{n} b_\ell 2^\ell \geq U$. Hence, if we had access to the true values of all b_i, we could obtain a 2-approximation to W.

We do not know true b_i values, but Lemma 1 shows that the M_i values computed by Algorithm 1 are sufficiently close to b_i with high probability. Recall that M_i is the median of MAP values computed by adding i random parity constraints and repeating the process T times. Specifically, for $c \geq 2$, it follows from Lemma 1 that for $0 < \alpha \leq \alpha^*(c)$,

$$\Pr\left[\bigcap_{i=0}^{n} \left(M_i \in [b_{\min\{i+c,n\}}, b_{\max\{i-c,0\}}] \right) \right] \geq 1 - n\exp(-\alpha T) \geq (1 - \delta)$$

for $T = \frac{\log(1/\delta)}{\alpha} \log n$, and $M_0 = b_0$. Thus, with probability at least $(1 - \delta)$ the output of Algorithm 1, $M_0 + \sum_{i=0}^{n-1} M_{i+1} 2^i$, lies in the range:

$$\left[b_0 + \sum_{i=0}^{n-1} b_{\min\{i+c+1,n\}} 2^i, b_0 + \sum_{i=0}^{n-1} b_{\max\{i+1-c,0\}} 2^i \right]$$

Let us denote this range $[L', U']$. By monotonicity of b_i, $L' \leq L \leq U \leq U'$. Hence, $W \in [L', U']$.

Applying Lemma 2, we have $U' \leq 2^{2c} L'$, which implies that with probability at least $1 - \delta$ the output of Algorithm 1 is a 2^{2c} approximation of W. For $c = 2$, observing that $\alpha^*(2) \geq 0.0042$ (see proof of Lemma 1), we obtain a 16-approximation for $0 < \alpha \leq 0.0042$. □

Proof of Theorem 2. As in the proof of Lemma 1, define the random variable

$$S_u(h^i_{A,b}) \triangleq \sum_{\sigma \in \{\sigma | w(\sigma) \geq u\}} 1_{\{A\sigma = b \bmod 2\}}$$

that gives the number of configurations with weight at least u satisfying i random parity constraints. Then for $i \leq \lfloor \log G(u) \rfloor - c \leq \log G(u) - c$ using Chebychev and Chernoff inequalities as in Lemma 1

$$\Pr\left[M_i \geq u\right] \geq 1 - \exp(-\alpha' T)$$

For $i \geq \lceil \log G(u) \rceil + c \geq \log G(u) + c$, using Chebychev and Chernoff inequalities as in Lemma 1

$$\Pr[M_i < u] \geq 1 - \exp(-\alpha' T)$$

Therefore,

$$\Pr\left[\frac{1}{2^{c+1}} 2^{q(u)} \leq G(u) \leq 2^{c+1} 2^{q(u)} \right] \geq$$
$$\Pr\left[\bigcap_{i=0}^{\lfloor \log_2 G(u) \rfloor - c} (M_i \geq u) \bigcap \left(M_{\lceil \log_2 G(u) \rceil + c} < u \right) \right] \geq$$
$$1 - n\exp(-\alpha' T) \geq 1 - \delta$$

This finishes the proof. □

Proof of Theorem 3. If $\widetilde{w}_i^t \leq w_i^t$, from Theorem 1 with probability at least $1-\delta$ we have $\widetilde{W} \leq M_0 + \sum_{i=0}^{n-1} M_{i+1} 2^i \leq UB'$. Since $\frac{UB'}{2^{2c}} \leq LB' \leq W \leq UB'$, it follows that with probability at least $1-\delta$, $\frac{\widetilde{W}}{2^{2c}} \leq W$.

If $w_i^t \geq \widetilde{w}_i^t \geq \frac{1}{L} w_i^t$, then from Theorem 1 with probability at least $1-\delta$ the output is $\frac{1}{L} LB' \leq \widetilde{W} \leq UB'$, and $LB' \leq W \leq UB'$. □