## 6. The perfect matching function

References:

- Alexander A. Razborov, A lower bound on the monotone network complexity of the logical permanent, Math. Notes Acad. Sci. USSR 37 (1985), 485–493.
- Stasys Jukna, Boolean Function Complexity: Advances and Frontiers, Springer 2012, 274–281.

The perfect matching function $PM_m$ is a monotone Boolean function of $n := m^2$ variables which correspond to the edge set of a bipartite graph $G = (A, B, E)$ where $|A| = |B| = m$. $PM_m(x) = 1$ iff the corresponding graph $G$ contains a perfect matching; i.e., a set of $m$ vertex-disjoint edges. Since a perfect matching in a given bipartite graph can be computed in polynomial time, the non-monotone complexity of $PM_m$ is also polynomial.

In 1985, Alexander Razborov has constructed approximators to prove an $m^{\Omega(\log m)}$ lower bound for the monotone network complexity of $PM_m$. As mentioned in their paper, Berg and Ulfberg have investigated the construction of DNF/CNF-approximators to prove a super-polynomial lower bound for the monotone net-

work complexity of $PM_m$.

Question:

Why Razborov-approximators suffice but DNF/CNF-approximators do not suffice to prove a super-polynomial lower bound for the monotone complexity of $PM_m$?

To get the possibility to answer this question, we shall investigate Razborov's proof.

Let $V = \{1,2,\dots,m\}$. $S_m$ denotes the set of all $m!$ permutations of $1,2,\dots,m$. Then we can write

$$PM_m(x) = \bigvee_{\sigma \in S_m} \bigwedge_{i=1}^{m} x_{i\sigma(i)}.$$

Goal:

Construction of a legitimate lattice $S = (S, \sqsubseteq, \neg)$ with large distance $\rho(PM_m, S)$.

Let

$$Per_\ell := \{ E' \subseteq A \times B \mid E' \text{ is a matching of size} \leq \ell \}.$$

Now we define $S$ exactly as above for the clique function where $Per_\ell$ plays the role of $V(\ell)$.

**Lemma 6.1**

$S = (S, \sqsubseteq, \sqcup)$ constructed above is a legitimate lattice.

**Proof:**

Exercise ∎

Let $G_+ = (A, B, E_+)$ be a random graph taking its values in the set of all $n!$ perfect matchings with equal probability $\frac{1}{n!}$.

Definition of $G_+ \Rightarrow$

$$\text{Prob}[\, PM_n(G_+) = 1 \,] = 1.$$

Let $h : A \cup B \to \{0,1\}$ be a random colouring assigning each node in $A \cup B$ a value 0 or 1 independently with probability $1/2$. This colouring defines a random graph $G_- = (V, E_-)$ where

$$V = A \cup B \text{ and } E_- = \{ (v,w) \mid h(v) = h(w) \}.$$

Note that in most cases, $G_-$ is not a bipartite graph.

**Lemma 6.2**

$$\text{Prob}[\, PM_n(G_-) = 0 \,] \geq 1 - \frac{2}{T_n}.$$

Proof:

The graph $G_- = (V, E_-)$ contains a perfect matching iff

$$\sum_{v \in A} h(v) = \sum_{w \in B} h(w). \quad \text{(show this!)}$$

$\Rightarrow$

$$\text{Prob}[PM_m(G_-) = 1] = \text{Prob}\left[\sum_{v \in A} h(v) = \sum_{w \in B} h(w)\right]$$

$$= \sum_{j=0}^{m} \text{Prob}\left[\sum_{v \in A} h(v) = j\right] \cdot \text{Prob}\left[\sum_{w \in B} h(w) = j\right]$$

$$\leq \max_{0 \leq j \leq m} \text{Prob}\left[\sum_{v \in A} h(v) = j\right]$$

$$\leq \binom{m}{\frac{m}{2}} \cdot 2^{-m} \leq \frac{2}{\sqrt{m}}$$

The last inequality is obtained using the Stirling formula.

Hence,

$$\text{Prob}[PM_m(G_-) = 0]$$

$$= 1 - \text{Prob}[PM_m(G_-) = 1]$$

$$\geq 1 - \frac{2}{\sqrt{m}}.$$

∎

Given any two members M and N of the lattice S, our goal is to show that the

probabilities $\mathrm{Prob}[G_+ \in \delta_\pi(N,N)]$ and $\mathrm{Prob}[G_- \in \delta_\pi(M,N)]$ are small. We shall consider $\mathrm{Prob}[G_+ \in \delta_\pi(N,M)]$ first.

Remember that $G_+$ is a random perfect matching.

**Lemma 6.3**

For any $M, N \in S$ there holds

$$\mathrm{Prob}[G_+ \in \delta_\pi(M,N)] \leq (r-1)^{2\ell} \cdot \frac{(m-\ell-1)!}{m!}.$$

**Proof:**

Let $M = \lceil A \rceil$ and $N = \lceil B \rceil$ where $A, B \subseteq \mathrm{Per}_\ell$ closed. Then

$$\begin{aligned}\delta_\pi(M,N) &= (\lceil A \rceil \cap \lceil B \rceil) \setminus \lceil A \rceil \cap \lceil B \rceil \\ &= (\lceil A \rceil \cap \lceil B \rceil) \setminus \lceil A \cap B \rceil.\end{aligned}$$

Let $A_m \subset A$ and $B_m \subset B$ denote the sets of minimal elements in $A$ and $B$, respectively. Then

$$\begin{aligned}\delta_\pi(M,N) &= (\lceil A_m \rceil \cap \lceil B_m \rceil) \setminus \lceil A \cap B \rceil \\ &= \Big( \bigcup_{E_1 \in A_m} \lceil E_1 \rceil \cap \bigcup_{E_2 \in B_m} \lceil E_2 \rceil \Big) \setminus \lceil A \cap B \rceil \\ &= \bigcup_{E_1 \in A_m} \bigcup_{E_2 \in B_m} (\lceil E_1 \rceil \cap \lceil E_2 \rceil) \setminus \lceil A \cap B \rceil\end{aligned}$$

Since $\lceil E_1 \rceil \cap \lceil E_2 \rceil = \lceil E_1 \cup E_2 \rceil$, we obtain

$$= \bigcup_{E_1 \in A_m} \bigcup_{E_2 \in B_m} (\lceil E_1 \cup E_2 \rceil \setminus \lceil A \cap B \rceil)$$

Consider any $E_1 \in A_m$, $E_2 \in B_m$. Then three cases are possible

Case 1: $E_1 \cup E_2$ is not a matching.

Then $\text{Prob}[G_+ \in \lceil E_1 \cup E_2 \rceil] = 0$

Case 2: $E_1 \cup E_2$ is a matching and $|E_1 \cup E_2| \leq \ell$.

Then $E_1 \cup E_2 \in \text{Per}_\ell$. $\Rightarrow$

- $A$ closed and $E_1 \in A \Rightarrow E_1 \cup E_2 \in A$
- $B$ closed and $E_2 \in B \Rightarrow E_1 \cup E_2 \in B$.

Hence, $E_1 \cup E_2 \in A \cap B$.

$\Rightarrow$ $\lceil E_1 \cup E_2 \rceil \setminus \lceil A \cap B \rceil = \emptyset$.

Case 3: $E_1 \cup E_2$ is a matching but $|E_1 \cup E_2| > \ell$.

$$\text{Prob}[G_+ \in \lceil E_1 \cup E_2 \rceil] = \text{Prob}[E_1 \cup E_2 \subseteq E_+]$$

$$= \frac{(m - |E_1 \cup E_2|)!}{m!}$$

$$\leq \frac{(m - \ell - 1)!}{m!}$$

Altogether, applying Lemma 4.3, we obtain

$$\text{Prob}[G_+ \in \delta_\Gamma(M, N)]$$

$$\leq |A_m| \cdot |B_m| \cdot \frac{(m-\ell-1)!}{m!}$$

$$\leq (r-1)^{2\ell} \cdot \frac{(m-\ell-1)!}{m!}$$

■

Since the events $e_1 \in E_-$ and $e_2 \in E_-$ are not necessarily independent, the proof of an upper bound for the probability $\text{Prob}[G_- \in \delta_v(M,N)]$ is more difficult. The following Lemma shows that these events are independent if the edges come from a fixed forest.

Lemma 6.4

Let $E' := \{(v_1,w_1),(v_2,w_2),\dots,(v_p,w_p)\} \subset A \times B$ be a forest F. Then the events $(v_i,w_i) \in E_-$ are independent, and each happens with probability $\frac{1}{2}$.

Proof:

Let $h: A \cup B \to \{0,1\}$ be a random coloring assigning each node in $A \cup B$ a value 0 or 1 independently with probability 1/2.

Assume that $h$ is performed in such an order that for each node $u$ unequal the root of a tree in F its father has been colored before.

For any edge $(v_i,w_i) \in E'$ consider the moment when the second node of $(v_i,w_i)$ is colored. Then

$(v_i,w_i) \in E_- \iff h(v_i) = h(w_i)$

This occurs with probability $\frac{1}{2}$ and do not depend on the fact if some other edges are in $E_-$ or not.

■

The following lemma shows that any subset $M \subseteq Per_e$ of $r$ pairwise disjoint matchings contains a large subset $M_0 \subseteq M$ such that the union of the matchings in $M_0$ is a forest.

Lemma 6.5

Let $M \subseteq Per_e$ be a set of $|M| = r$ pairwise disjoint matchings. Then there exists a subset $M_0 \subseteq M$ of $|M_0| \geq \frac{\sqrt{r}}{e}$ matchings such that $\bigcup_{A \in M_0} A$ is a forest.

Proof:

Let $M_0 \subseteq M$ such that $\bigcup_{A \in M_0} A$ is a forest and $|M_0|$ is maximal.

It suffices to show that $|M_0| \geq \frac{\sqrt{r}}{e}$.

Assume that $|M_0| < \frac{\sqrt{r}}{e}$. Let $E_0 := \bigcup_{A \in M_0} A$.

$\Rightarrow$

$$|E_0| < \sqrt{r}.$$

Let $A_0 \subseteq A$ and $B_0 \subseteq B$ be the sets of nodes which are end node of at least one edge in $E_0$.

$\Rightarrow$

$$|A_0| < \sqrt{r} \quad \text{and} \quad |B_0| < \sqrt{r}.$$

Since $M$ contains $|M| = r > |A_0 \times A_0|$ pairwise disjoint matchings at least one of

these matchings, say $A_1$, contains no edge in $A_0 \times B_0$.

Since $A_1$ is a matching and $E_0$ is a forest lying in $A_0 \times B_0$, the graph $E_0 \cup A_1$ is a forest as well.

But $A_1 \cap E_0 = \emptyset$ implies $A_1 \notin M_0$, a contradiction to the maximality of $|M_0|$.

■

Note that

$$|Perf_\ell| \leq \sum_{i=0}^{\ell} \binom{m}{i}^2 \cdot i! \leq m^\ell \sum_{i=0}^{\ell} \binom{m}{i} \leq m^{2\ell}.$$

Now we are prepared to prove an upper bound for $Prob[G_- \in \delta_\sqcup(M,N)]$

Lemma 6.6

For any $M, N \in S$, there holds

$$Prob(G_- \in \delta_\sqcup(M,N)) \leq (1-2^{-k})^{\lceil r/k \rceil} \cdot 2r^\ell$$

Proof:

Let $M = \lceil A \rceil$, $N = \lceil B \rceil$ and $C = A \cup B$.

$\Rightarrow$

$$\delta_\sqcup(M,N) = \lceil C^* \rceil \setminus C.$$

Let $C = C_0, C_1, C_2, \ldots, C_p = C^*$ be the results of the improvement steps in the construction of $C^*$ from $C$.

Let $W_i \in \{W \notin C_{i-1} \mid C_{i-1} \vdash W\}$ be the chosen set for the construction of $C_i$ from $C_{i-1}$.

Since $p \leq 2r^\ell$ it suffices to prove that

(*) $\text{Prob}[G_- \in \lceil C_i \rceil \setminus \lceil C_{i-1} \rceil] \leq (1-2^{-\ell})^{\frac{r}{\ell}}$.

Let $A_1, A_2, \ldots, A_r \in C_{i-1} : A_1, A_2, \ldots, A_r \vdash W$.

Definition of $\vdash \Rightarrow$

$A_1 \setminus W, A_2 \setminus W, \ldots, A_r \setminus W$ are pairwise disjoint matchings in $\text{Per}_\ell$.

If at least one of these matchings is empty then a subset of $W$ would be contained in $C_{i-1}$ and hence, $\lceil W \rceil \subseteq \lceil C_{i-1} \rceil$. By construction, $\lceil C_i \rceil = \lceil C_{i-1} \rceil$ such that (*) trivially holds.

Otherwise, applying Lemma 6.5, we choose a subset $M_0 \subseteq \{A_1 \setminus W, A_2 \setminus W, \ldots, A_r \setminus W\}$ such that $\bigcup_{A \in M_0} A$ is a forest and $|M_0| \geq \frac{r}{\ell}$.

$\Rightarrow$

$$\begin{aligned}
&\text{Prob}[G_- \in \lceil C_i \rceil \setminus \lceil C_{i-1} \rceil] \\
&\leq \text{Prob}[W \subseteq E_- \text{ and } A_i \not\subseteq E_- \; \forall i = 1, \ldots, r] \\
&\leq \text{Prob}[A_i \setminus W \not\subseteq E_- \; \forall i = 1, \ldots, r] \\
&\leq \text{Prob}[A_i \setminus W \not\subseteq E_- \; \forall A_i \setminus W \in M_0]
\end{aligned}$$

Lemma 6.4 $\Rightarrow$

All events $A_i \setminus W \subseteq E_-$ for $A_i \setminus W \in M_0$ are independent and

$$\text{Prob}[A_i \setminus W \subseteq E_-] = 2^{-|A_i \setminus W|} \geq 2^{-\ell}.$$

Therefore,

$$\text{Prob}[A_i|W \subseteq E_- \;\forall\, A_i|W \in M_0] = \prod_{A_i|W \in M_0} \text{Prob}[A_i|W \notin E_-] \leq (1-2^{-\ell})^{\frac{r}{\ell}}$$

**Theorem 6.1**

$$C_{\Omega_m}(PM_m) \geq m^{\Omega(\log m)}$$

**Proof:**

Let $t = \varrho(PM_m, S)$ where $\ell := \lfloor \frac{1}{8} \log m \rfloor$ and $r := \lfloor m^{1/4} \log^8 m \rfloor$.

Consides $M, M_1, N_1, M_2, N_2, \ldots, M_t, N_t \in S$ such that

$$\sigma(PM_m) \subseteq M \cup \bigcup_{i=1}^{t} \delta_r(M_i, N_i)$$

and

$$M \subseteq \sigma(PM_m) \cup \bigcup_{i=1}^{t} \delta_u(M_i, N_i).$$

We distinguish two cases.

Case 1: $M = \emptyset$.

Then $\sigma(\emptyset) \subseteq \bigcup_{i=1}^{t} \delta_r(M_i, N_i)$.

Since $G_+ \in \sigma(PM_m)$ with probability 1, the sum of probabilities $\text{Prob}(G_+ \in \delta_r(M_i, N_i))$

at least 1 as well. Hence, by Lemma 6.3

$$t \cdot (r-1)^{2e} \frac{(m-e-1)!}{m!} \geq 1$$

$$\Leftrightarrow \quad t \geq \frac{m!}{(m-e-1)!\,(r-1)^{2e}}$$

$$\geq \left(\frac{m}{2}\right)^{e} r^{-2e}$$

$$= \left(\frac{m}{2r^2}\right)^{e}$$

$$\geq \left(\frac{m}{2\,(m^{1/2}\log^{16} m)}\right)^{\frac{\log m}{8}}$$

$$= m^{\Omega(\log m)}$$

Case 2: $M \neq \emptyset$.

Then $\exists\, A \in Per_e$ such that $\lceil A \rceil \subseteq M$

$\Rightarrow$

$$\lceil A \rceil \subseteq \sigma(PM_m) \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i)$$

Lemma 6.4 $\Rightarrow$

$$\text{Prob}(G_- \in \lceil A \rceil) = 2^{-|A|} \geq 2^{-e}$$

Lemma 6.2 $\Rightarrow$

$$\text{Prob}(G_- \in \sigma(PM_m)) \leq 2 \cdot m^{-1/2}$$

Lemma 6.6 $\Rightarrow$

$$\text{Prob}(G_- \in \delta_{\sqcup}(M_i, N_i)] \leq (1-2^{-e})^{\frac{r-1}{e}} \cdot 2r^e$$

$$\leq (1-2^{-e})^{\frac{r}{e}} \cdot m^{2e}$$

Hence we obtain

$$t \geq (2^{-\ell} - 2m^{-1/2})(1 - 2^{-\ell})^{-\frac{\sqrt{r}}{\ell}} m^{-2\ell}$$

Since $1 - x \geq e^{-x - \frac{x^2}{2}}$ for $0 < x < 1$ we obtain

$$\begin{aligned} t &\geq (2^{-\ell} - 2m^{-1/2})\, e^{2^{-\ell}\frac{\sqrt{r}}{\ell} + \underbrace{2^{-2\ell}\cdot\frac{\sqrt{r}}{\ell}}_{\to 0}} \cdot m^{-2\ell} \\ &\geq (2^{-\ell} - 2m^{-1/2})\, e^{2^{-\ell}\cdot\frac{\sqrt{r}}{\ell}} \cdot m^{-2\ell} \\ &\geq \tfrac{1}{8} m^{-\frac{1}{8}} \cdot e^{2^{-\ell}\cdot\frac{\sqrt{r}}{\ell}} \cdot m^{-2\ell} \\ &\geq \tfrac{1}{8} m^{-1/8 - 1/4 \log m} \cdot e^{\frac{8\cdot m^{-\frac{1}{8}}\cdot m^{\frac{1}{8}}\cdot \log^4 m}{\log m}} \\ &= m^{-\Omega(\log^2 m)} \end{aligned}$$

This proves the theorem. ∎

Let us return to our former question:

Why Razborov-approximators suffice but DNF/CNF-approximators do not suffice to prove a super-polynomial lower bound for the monotone complexity of $PM_m$?

Knowing Razborov's solution, it is still difficult to answer the above question. First, one could try to use Razborov's test sets and his arguments to prove the needed lemmas with respect to DNF/CNF-approximators.

To continue at page 186.