A semantic view of the switching lemma

Dimitris J. Kavvadias and Lina Panagopoulou

Department of Mathematics
University of Patras

June 17, 2018

Overview

The Switching Lemma

- Deals with boolean functions
- Boolean function φ: defined on *n boolean variables* using the *logical connectives* ($\vee$, $\wedge$, $\neg$)
- $\varphi : \{0,1\}^n \to \{0,1\}$
- φ may come in various syntactic forms
  - Conjuctive normal form, CNF
    - kCNF: each clause has at most k literals
      $\varphi = (\neg x_1 \vee \neg x_2 \vee x_5) \wedge (x_2 \vee \neg x_4 \vee x_5) \wedge (\neg x_3 \vee x_4) \wedge (x_4 \vee \neg x_5)$
  - Disjuctive normal form, DNF
    - kDNF: each term has at most k literals
      $\varphi = (x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_3 \wedge x_4) \vee (x_2 \wedge \neg x_4)$

The Switching Lemma

- Let φ be a boolean function in CNF
- Random restriction ρ: select each variable with probability p and assign to it the value 0 or 1 with probability 0.5
- p is close to 1
- $\varphi|_\rho$ is the simplified function after substituting the chosen values to the selected variables
- Example:
  $\varphi = (\neg x_1 \vee \neg x_2 \vee x_5) \wedge (x_2 \vee \neg x_4 \vee x_5) \wedge (\neg x_3 \vee x_4) \wedge (x_4 \vee \neg x_5)$
  Let $\rho : x_1 = 0, x_3 = 1, x_5 = 0$
  Then $\varphi|_\rho = (x_2 \vee \neg x_4) \wedge (x_4)$

The Switching Lemma

- The Switching Lemma: If φ is kCNF then $\varphi|_\rho$ is sDNF expressible with high probability for constants $k, s \geq 2$.

Switching Lemma (Håstad 1986)

Let φ be a kCNF expressible Boolean function. Let ρ be a random restriction that selects a variable of φ with probability p. Then for every $s \geq 2$.

$$\Pr(\varphi\,|_\rho \text{ is not } s\text{DNF expressible}) \leq (5k(1-p))^s$$

- De Morgan's rule gives a symmetric form of the Switching Lemma

Applications of the Switching Lemma

- Parity function.
  For $x_i \in \{0,1\}^n$ $f(x_1, x_2, \ldots, x_n) = \Sigma_{i=1}^{n} x_i \pmod 2$

- The parity function cannot be computed by constant depth, unbounded fan-in, polynomial size circuits

Proofs of the Switching Lemma

- M. Ajtai
- A. C. C. Yao
- M. Furst, J. Saxe and M. Sipser
- J. Håstad 1986: using quite involved arguments with conditional probabilities
- A. Razborov 1992: simpler proof using information-theoretic arguments
- P. Beame 1994: simplified arguments using decision trees

All the above are based on studying the effects of the restriction on the formula φ itself (syntactic approach)

A semantic view of the Switching Lemma

- Instead of studying the formula φ, we study its set of *models* M i.e., satisying truth assignments

Definition $k-$compatibility

Let n be a positive integer and let $M \subseteq \{0,1\}^n$ be a set of Boolean vectors. For $k > 1$, we say that a Boolean vector $v \in \{0,1\}^n$ is k-compatible with M if for any sequence of k positions $0 \leq i_1 < \ldots < i_k \leq n$, there exists a vector in M that agrees with v in these k positions.

A semantic view of the Switching Lemma

Lemma kCNF expressibility

Let $M \subseteq \{0,1\}^n$ be a set of binary vectors. Then the following are equivalent:

- M is a kCNF set.
- If $m \in \{0,1\}^n$ is k-compatible with M, then $m \in M$

- De Morgan's rule leads to symmetric form

Lemma kDNF expressibility

Let $M \subseteq \{0,1\}^n$ be a set of binary vectors. Then the following are equivalent:

- M is a kDNF set.
- If $m \in \{0,1\}^n$ is k-compatible with $\overline{M}$, then $m \in \overline{M}$

A semantic view of the Switching Lemma

- In the vector view
  - A random restriction ρ selects a subset of vectors of M that agree with the chosen values in the selected positions by ρ
  - The fixed positions by ρ are projected out
- Let N be the remaining parts of the chosen vectors. Define $M|_{\rho} = N$
- Informally: if M is kCNF then with high probability N is sDNF for $k, s \geq 2$

A semantic view of the Switching Lemma

- Combining the above

The Switching Lemma (semantic form)

Let $M \subseteq \{0,1\}^n$ be a set of binary vectors with the property that every vector $m \in \overline{M}$ is not k-compatible with M. Let ρ be a random restriction on M that selects a position with probability p and let $N = M|_{\rho}$. Then for every $s \geq 2$.

$$\Pr(N \text{ includes an } s\text{-compatible vector with } \overline{N}) \leq (5k(1-p))^s$$

A semantic view of the Switching Lemma

- M is kCNF set: every model in $\overline{M}$ has specific "bad" values in at least one "bad" $k-$tuple of positions
- This k-tuple corresponds to a clause C.
- With respect to a specific bad $k-$tuple, a random restriction ρ may:
  1. Select all k positions of the tuple with bad values. This corresponds to falsifying clause C. $\Pr(C \equiv 0) = (\frac{p}{2})^k$
  2. Select at least one "good" value in the $k-$tuple. This corresponds to satisfying clause C. $\Pr(C \equiv 1) = 1 - (1 - \frac{p}{2})^k$
  3. Select up to $k-1$ positions with bad values. The bad tuple remains possibly with smaller k. Clause C "survives". $\Pr(C \text{ survives from } \rho) = P_s = (1 - \frac{p}{2})^k - (\frac{p}{2})^k$

A semantic view of the Switching Lemma

- Observation. The three previous cases correspond to:
  1. ρ falsifies C, $M|_\rho$ is empty, trivially sDNF. ρ is a good restriction
  2. ρ satisfies C, C is removed from the formula
  3. The interesting case. C remains in the formula but possibly becomes smaller

Lemma

If $\ell \leq s$ bad tuples survive the restriction ρ then ρ is a good restriction.

- Idea: the above case a disagreeing $s-$tuple can always be found for every model in N

A semantic view of the Switching Lemma

- If $\ell > s$ tuples survive then ρ can be either good or bad
- Special case. Disjoint clauses
- In this case when $\ell > s, \rho$ is bad
- The exact probability can now be calculated
- Let m be the number of clauses of φ

$$\Pr(\varphi\,|\,_\rho \text{ is not } s\text{DNF})) = (1-(\frac{p}{2})^k)^m - \sum_{j=0}^{s} \binom{m}{j} \cdot P_s^j \cdot (1-(1-\frac{p}{2})^k)^{m-j}$$

Sketch of proof

- General case: the clauses are not disjoint
- We consider the case $\ell > s$ to give a bad restriction
- Proof by induction on m, the number of clauses
- Denote by $H_s = 5k(1-p)^s$
- Let $e(\varphi, s)$ the event that exactly $\ell = s$ clauses survive in $\varphi|_\rho$
- Let $E(\varphi, s)$ the event that $\ell > s$ clauses survive in $\varphi|_\rho$
- Denote $\varphi' = \varphi \backslash C$

Sketch of proof

Inductive relation

$$\Pr(E(\varphi, s)) = \Pr(e(\varphi', s) \wedge (C \text{ survives})) + \Pr(E(\varphi', s) \wedge (C \not\equiv 0))$$

- This relation allows induction on the number of clauses
- Inductive hypothesis. Assume $\Pr(E(\varphi, s)) \leq H_s$
- We restrict our attention to the set of assignments $\mathcal{A}$ that make C survive
- For $\alpha \in \mathcal{A}$ let $e(\alpha)$ be the event: ρ assigns α to the variables of C

Sketch of proof

- First term becomes

$$\Pr(e(\varphi', s) \wedge (C\ \mathit{survives})) =$$
$$\Pr(e(\varphi', s) \wedge \bigvee_{\alpha \in \mathcal{A}} e(\alpha)) = \Pr(\bigvee_{\alpha \in \mathcal{A}} (e(\varphi', s) \wedge e(\alpha))) \leq$$
$$\sum_{\alpha \in \mathcal{A}} \Pr(e(\varphi', s) \wedge e(\alpha)) \leq \sum_{\alpha \in \mathcal{A}} \Pr(E(\varphi', s-1) \wedge e(\alpha)) =$$
$$\sum_{\alpha \in \mathcal{A}} \Pr(E(\varphi', s-1) \mid e(\alpha)) \cdot \Pr(e(\alpha))$$

Sketch of proof

- Using the induction hypothesis we get

$$\Pr(E(\varphi', s-1) \mid e(\alpha)) \leq H_{s-1}$$

- Note. There are issues involving conditioning on $e(\alpha)$
- First term becomes

$$\Pr(e(\varphi', s) \wedge (C \textit{ survives})) \leq H_{s-1} \sum_{\alpha \in \mathcal{A}} \Pr(e(\alpha)) = H_{s-1} P_s$$

Sketch of proof

- We do the same for the second term and get that

$$\Pr(\varphi|_\rho \text{ is not } s\text{DNF}) \leq H_{s-1}P_s + H_s(1-(\frac{p}{2})^k)$$

- To complete the induction we need to show

$$H_{s-1}P_s + H_s(1-(\frac{p}{2})^k) \leq H_s$$

- or equivalently

$$\left(1-\frac{p}{2}\right)^k \leq (5k(1-p)+1)\left(\frac{p}{2}\right)^k$$

- This can be shown by algebraic manipulations

The End