Pseudo-partitions, Transversality and Locality: A Combinatorial Characterization for the Space Measure in Algebraic Proof Systems.

Ilario Bonacina and Nicola Galesi

Rome, 27 September 2012

About this talk

In this talk:

- Combinatorial characterization of space in PCR (Main Theorem) via k-extendibility/winning strategies
- Ideas behind the winning strategy for random kCNF

Let V a set of variables and $P \subset \mathbb{F}[V]$ contradictory (i.e. $1 \in \langle P \rangle$).

PC/PCR Derivation Rules

$$\frac{p \qquad q}{\alpha p + \beta q} \forall \alpha, \beta \in \mathbb{F}, \qquad \frac{p}{xp} \forall x \in V \qquad \frac{}{x^2 - x} \forall x \in V.$$

in PCR: $V = \{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$ and $x_i + \overline{x_i} - 1 \in P$.
$\pi = (C_0, \ldots, C_l)$ is a *proof* of $P \vdash 1$ iff

- each C_i is a set of polynomials (memory configuration); $C_0 = \emptyset$, $C_l = \{1\}$,
- $\mathcal{C}_i$ derive from $\mathcal{C}_{i-1}$ by an axiom download (adding to C_{i-1} a polynomial from P) or by applying a derivation rule to polynomials in C_{i-1} or by erasing some polynomial in C_{i-1}.

$Sp(\pi) = \max_i\{\#$ of distinct monomials in $\mathcal{C}_i\}$.
$Sp(P) = \min_\pi\{Sp(\pi) : \pi$ is a proof of $P \vdash 1\}$ (Monomial Space).

Theorem (ABRW02)

$Sp(CT_n) \geq n/4$, $Sp(PHP_n^m) \geq n/4$ and more in general for "wide" CNF in some multivalued logic.

Theorem (FLNTZ12)

$Sp(BPHP_n^m) \geq n/8$, $Sp(XPHP_n^m) \geq n/4$.

Theorem (Main Theorem)

Let P be a contradictory set of polynomials (i.e $1 \in \langle P \rangle$) and I a proper ideal. If there exists a non-empty k-extendible family of admissible configurations $\mathcal{F}$ for P with respect to I. Then $Sp(P) \geq k/4$.

Corollaries:

- $Sp(CT_n) \geq n/4$, $Sp(PHP_n^m) \geq n/4$, $Sp(BPHP_n^m) \geq n/8$, $Sp(XPHP_n^m) \geq (n-1)/4$.
- Let $k \geq 4$ be any integer, $k - 3 > \epsilon > 0$ any constant and $\Delta \geq 1$. Let $F \sim \mathcal{F}(n, \Delta, k)$ a random kCNF. There exists a constant $c = c_{k,\Delta,\epsilon}$, $c \geq 1$, such that with high probability $Sp(F) \geq \frac{n}{4c}$.
- There exists a constant degree $d \geq 3$ bipartite graph $\mathcal{G} = (U \cup V, E)$ with $|U| = n + 1$ and $|V| = n$, such that $Sp(\mathcal{G}\text{-}PHP) \geq \Omega(n/d)$.

Preliminary Definitions

Let V a set of variables, $\mathbb{F}[V]$ a ring of polynomials, $P \subseteq \mathbb{F}[V]$ a set of contradictory polynomials, $I \subset \mathbb{F}[V]$ a proper ideal.

(partial assignment) $\alpha : V \longrightarrow \{0, 1, \star\}$.

(pseudo-partition) $\mathcal{Q} = \{Q_1, \ldots, Q_t\}$, where each $Q_i \subseteq V$ and they don't overlap.

($\mathcal{Q}$-lm family) $\mathcal{H} = H_1 \times \ldots \times H_t$, where each H_i is a set of partial assignments with domain Q_i st

1. $\forall x \in Q_i \ \exists \alpha_0, \alpha_1 \in H_i$ st $\alpha_1(x) = 1$, $\alpha_0(x) = 0$,
2. $\forall p \in I \ \forall \alpha \in H_i \ \alpha \models_I p$.

($\models_I$ for polynomials) $\alpha \models_I p$ iff $\alpha(p) \in I$,

(admissible configurations) pairs $(\mathcal{Q}, \mathcal{H})$ "$\mathcal{H}$ is $\mathcal{Q}$-lm"

(the ordering $\preceq$) $(\mathcal{Q}, \mathcal{H}) \preceq (\mathcal{Q}', \mathcal{H}')$ iff (1) $\mathcal{Q} \subseteq \mathcal{Q}'$, and (2) $\mathcal{H}' \restriction_{\mathcal{Q}} = \mathcal{H}$.

k-Extendibility/Winning Strategies

A non-empty family $\mathcal{F}$ of admissible configurations $(\mathcal{Q}, \mathcal{H})$ is *k-extendible* for P with respect to I iff

1. $|\mathcal{Q}| \leq k$,
2. $\forall \mathcal{Q}' \subseteq \mathcal{Q} \ \ (\mathcal{Q}', \mathcal{H}{\restriction_{\mathcal{Q}'}}) \in \mathcal{F}$.
3. if $|\mathcal{Q}| < k$, then $\forall a \in P \ \ \exists (\mathcal{Q}', \mathcal{H}') \in \mathcal{F}$ st
   - $(\mathcal{Q}, \mathcal{H}) \preceq (\mathcal{Q}', \mathcal{H}')$,
   - $\mathcal{H}' \models_I a$,
   - $|\mathcal{Q}'| \leq |\mathcal{Q}| + 1$.

Theorem (Main Theorem)

Let P be a contradictory set of polynomials (i.e $1 \in \langle P \rangle$) and I a proper ideal.
If there exists a non-empty k-extendible family of admissible configurations $\mathcal{F}$ for P with respect to I. Then the $Sp(P) \geq k/4$.

(transversal 2CNF) M is a 2CNF transveral to $\mathcal{Q}$ pseudo-partition iff M is a 2CNF and $Var(M)$ hits each element of $\mathcal{Q}$ exactly once.

($\models_I^{(\mathcal{Q},\mathcal{H})}$) $M \models_I^{(\mathcal{Q},\mathcal{H})} p$ iff M is transversal to $\mathcal{Q}$, $\mathcal{H}$ is $\mathcal{Q}$-lm with respect to I and $\forall \alpha \in \mathcal{H}$ $(\alpha \models M \longrightarrow \alpha \models_I p)$.

(main induction on i) $\pi = (C_1, \ldots, C_s)$ a refutation of P in PCR and by contradiction $Sp(\pi) < k/4$.

1. $M_i \models_I^{(\mathcal{Q}^i,\mathcal{H}_i,)} C_i$,
2. $|M_i| \leq 2Sp(C_i)$,
3. $(\mathcal{Q}^i, \mathcal{H}_i) \in \mathcal{F}$.

Lemma (Locality Lemma)

Let T be a set of polynomials, $\mathcal{Q}$ a pseudo-partition and $\mathcal{H}$ a $\mathcal{Q}$-lm family of assignments. Let M be a 2CNF transversal to $\mathcal{Q}$. If $M \models_I^{(\mathcal{Q},\mathcal{H})} p$, then there exists a pseudo-partition $\mathcal{Q}' \subseteq \mathcal{Q}$ and there exists a 2CNF M' transversal to $\mathcal{Q}'$ such that:

- $M' \models_I^{(\mathcal{Q}',\mathcal{H}\restriction_{\mathcal{Q}'})} P$ *and*
- $|M'| \leq 2Sp(p)$.

Proof somehow similar to the one in ABRW02.

Winning Strategy for Random kCNF (Sketch)

Let $\mathcal{G} = (U \cup V, E)$ the natural bipartite graph we can associate to a random kCNF.

Definition ((r, s)-double matching property)

Let $r \leq s$, $A \subseteq U$ of size at most r and $B \subseteq V \cap N_{\mathcal{G}}(A)$. We say that $(\mathcal{G}, A, B)$ has the (r, s)-double matching property if for every $C \subseteq U \setminus A$, if $|C| = s - |A|$ then there exists a 2-matching of C into $V \setminus B$.

For $k \geq 4$ a standard union bound shows that the graph $\mathcal{G}$ with high probability has this expansion property

$$\forall A \subseteq U,\ |A| \leq s \longrightarrow |N_{\mathcal{G}}(A)| \geq (2 + \epsilon)|A|,$$

where $s = \Omega(n)$. For some $\tilde{r} = s/c$ this allows us to dinamically maintain the $(\tilde{r}, s)$-double matching property. This leads to the $\tilde{r}$-extendibility property for the random kCNF with respect to the ideal generated by the logical axioms.

Further Directions/Open Problems

- improve Locality Lemma
- Random 3CNF
- Tseitin tautologies or other noticeable families
- Variable Space
- link with degree (similar to the approach of Atserias and Dalmau for Resolution)
- characterization by E.F. games?
- extend this techniques to other proofs systems

Thank You! ...Questions?