From Treelike Res($\oplus$) to $\mathbb{F}_2$-Nullstellensatz

S. Bianco

May 26, 2024

Contents

1 The $\frac{1}{3}, \frac{2}{3}$ lemma

Definition 1. Given a tree T and a node v, we denote as T_v the subtree of T having v as its radix.

Lemma 1 (Lewis' $\frac{1}{3}, \frac{2}{3}$ lemma [LSH65])**.** *If T is a binary tree of size $s > 1$ then there is a node v such that the subtree T_v has size between $\left\lfloor \frac{1}{3}s \right\rfloor$ and $\left\lceil \frac{2}{3}s \right\rceil$.*

Proof. Let r be the radix of T and let ℓ be a leaf of T with the longest possible path $r \to \ell$. Let $v_1, \ldots, v_k$ be the nodes of such path, where $r = v_1$ and $\ell = v_k$. For each index i such that $1 \leq i \leq k$, let $a_i b_i$ be the two children of v_i.

Claim 1.1. For any index i, if T_{v_i} has size at least $\left\lfloor \frac{1}{3}s \right\rfloor$ then for some index j, where $i \leq j \leq k$, it holds that T_{v_j} has size between $\left\lfloor \frac{1}{3}s \right\rfloor$ and $\left\lceil \frac{2}{3}s \right\rceil$.

Proof of the claim. If T_{v_i} has also size less than $\left\lceil \frac{2}{3}s \right\rceil$ then we are done. Otherwise, since $T_{v_i} = \{v_i\} \cup T_{a_i} \cup T_{b_i}$, one between the subtrees T_{a_i}, T_{b_i} must have size at least $\frac{1}{2} \lceil 2 \rceil 3s - 1$, meaning that it has size at least $\left\lfloor \frac{1}{3}s \right\rfloor$. If this subtree has also a size at most $\left\lceil \frac{2}{3}s \right\rceil$ then we are done. Instead, if this doesn't hold for both subtrees, we can repeat the process (assuming that $v_{i+1} := a_i$ without loss of generality) since we know that $T_{v_{i+1}}$ has size greater than $\left\lfloor \frac{1}{3}s \right\rfloor$.

By way of contradiction, suppose that this process never finds a subtree with size at most $\left\lceil \frac{2}{3}s \right\rceil$. Then, this would mean that it also holds for $v_k = \ell$. However, since ℓ is a leaf, we know that T_{v_ℓ} must have size 1, which is definitely at most $\left\lceil \frac{2}{3}s \right\rceil$ for any value of s, giving a contradiction. Thus, there must be a node that terminates the process.

□

Since $T_{v_1} = \{r\} \cup T_{a_1} \cup T_{b_1}$, we know that for both of these subtrees must have at least $\left\lfloor \frac{1}{3}s \right\rfloor$. Thus, assuming that $a_1 = v_2$, the claim directly concludes the proof.

□

2 Nullstellensatz

Definitions taken from [DMN+21]

Definition 2 (Hilbert's Nullstellensatz)**.** Given the polynomials $p_1, \ldots, p_m \in \mathbb{F}[x_1, \ldots, x_n]$, the equation $p_1 = \ldots = p_m = 0$ is unsolvable if and only if $\exists g_1, \ldots, g_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\sum_{i=1}^{m} g_i p_i = 1$.

Hilbert's Nullstellensatz can be used to define the following proof system:

Definition 3 (Nullstellensatz Refutation)**.** Given the set of polynomial equations $P = \{p_1 = 0, \ldots, p_m = 0\}$ over $\mathbb{F}[x_1, \ldots, x_n]$, where $\mathbb{F}$ is any field, a Nullstellensatz refutation is a set of polynomials $\pi = \{g_1, \ldots, g_n\} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that $\sum_{i=1}^{m} g_i p_i = 1$.

The set of polynomials $P = \{p_1, \ldots, p_n\}$ is called the axiom set and the set $\pi = \{g_1, \ldots, g_n, h_1, \ldots, h_m\}$ is called proof of P.

By also adding the polynomial equations $x_1^2 - x_1 = 0, \ldots, x_n^2 - x_n = 0$ to the set of axioms, the NS proof system is sound and complete for the set of unsatisfiable CNF formulas. Thus, in general, given the set of axioms $P = \{p_1 = 0, \ldots, p_m = 0, x_1^2 - x_1 = 0, \ldots, x_n^2 - x_n = 0\}$, we say that $\pi = \{g_1, \ldots, g_m, h_1, \ldots, h_n\}$ is a CNF proof of P if:

$$\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = 1$$

For any proof $\pi = \{g_1, \ldots, g_n, h_1, \ldots, h_m\}$ of the axioms $P = \{p_1, \ldots, p_n\}$, we define the *degree of* π as:

$$\deg(\pi) = \max\{\deg(g_i p_i), \deg(h_j) + 2 \mid 1 \leq i \leq n, 1 \leq j \leq m\}$$

If P has a proof π of degree $\deg(\pi) = d$ then we say that $P \vdash_d^{\mathsf{NS}} 1$.

Proposition 1. *Given a set of axioms P, if $P \vdash_d^{\mathsf{NS}} q$ then $P, 1 - q \vdash_d^{\mathsf{NS}} 1$*

Proof. Since $P \vdash_d^{\mathsf{NS}} q$, we know that $\exists g_1, \ldots, g_m, h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that:

$$\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = q$$

where $\deg(q) = d$.

Let $p_{m+1} := 1 - q$ and $P' = P \cup \{p_{m+1} = 0\}$. We define $g'_1, \ldots, g'_m, g'_{m+1}$ as:

$$g'_i = \begin{cases} 1 & \text{if } i = m+1 \\ g_i & \text{otherwise} \end{cases}$$

With simple algebra we get that:

$$\sum_{i=1}^{m+1} g'_i p_i + \sum_{j=1}^{n} h_j(x_j^2 - x_j) = g'_{m+1} p_{m+1} + \sum_{i=1}^{m} g'_i p_i + \sum_{j=1}^{n} h_j(x_j^2 - x_j) = (1-q) + q = 1$$

thus $\pi = \{g'_1, \ldots, g'_{m+1}, h_1, \ldots, h_n\}$ is a proof of P. Moreover, since $\deg(q) = d$ implies that $\deg(g'_{m+1} p_{m+1}) = d$, it's easy to see that $\deg(\pi) = d$ holds, concluding that $P, 1 - q \vdash_d^{\mathsf{NS}} 1$

$\square$

Lemma 2. *Given two disjoint axiom sets* P_1, P_2, *if* $P_1, p \vdash_{d_1}^{\mathsf{NS}} 1$ *and* $P_2, 1 - p \vdash_{d_2}^{\mathsf{NS}} 1$ *then* $P_1, P_2 \vdash_{d_1+d_2}^{\mathsf{NS}} 1$.

Proof. Suppose that $P_1 = \{p_1, \ldots, p_m\}$ and $P_2 = \{q_1, \ldots, q_k\}$. Let $p_{m+1} = p$ and let $q_{k+1} = 1 - p$. By hypothesis, we know that

$$\sum_{i=1}^{m+1} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j) = 1$$

for some $g_1, \ldots, g_{m+1}, a_1, \ldots, a_n$, implying that:

$$\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j) = 1 - g_{m+1} p_{m+1} = 1 - g_{m+1} p$$

Likewise, we know that:

$$\sum_{i=1}^{k+1} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j) = 1$$

for some $r_1, \ldots, r_{k+1}, b_1, \ldots, b_n$, implying that:

$$\sum_{i=1}^{k} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j) = 1 - r_{k+1} q_{k+1} = 1 - r_{k+1}(1 - p)$$

We notice that:

$$
\begin{aligned}
(1-p)\left(\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j)\right) &= (1-p)(1-g_{m+1}p) \\
&= 1 - g_{m+1}p - p + g_{m+1}p^2 \\
&= 1 - p
\end{aligned}
$$

In the last step, we used the fact that, due to multilinearity, it holds that $p^2 = p$. Proceeding the same way, we find that:

$$
\begin{aligned}
p\left(\sum_{i=1}^{k} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j)\right) &= p\left(1 - r_{k+1}(1-p)\right) \\
&= p\left(1 - r_{k+1} + r_{k+1}p\right) \\
&= p - r_{k+1}p + r_{k+1}p^2 \\
&= p
\end{aligned}
$$

Now, we define $s_1, \ldots, s_{m+k}$

$$
s_i = \begin{cases} g_i \cdot (1-p) & \text{if } 1 \leq i \leq m \\ r_i \cdot p & \text{if } m+1 \leq i \leq k \end{cases}
$$

and $h_1, \ldots, h_n$ as $h_j = a_j \cdot (1-p) + b_j \cdot p$.

At this point, through simple algebra we get that:

$$
\sum_{i=1}^{m+k} s_i p_i + \sum_{j=1}^{n} h_j(x_j^2 - x_j) =
$$

$$
(1-p)\left(\sum_{i=1}^{m} g_i p_i + \sum_{j=1}^{n} a_j(x_j^2 - x_j)\right) + p\left(\sum_{i=1}^{k} r_i p_i + \sum_{j=1}^{n} b_j(x_j^2 - x_j)\right) =
$$

$$
(1-p)(1-g_{m+1}p) + p\left(1 - r_{k+1}(1-p)\right) = p + 1 - p = 1
$$

concluding that $\pi_3 = \{s_1, \ldots, s_{m+k}, h_1, \ldots, h_n\}$ is a proof of $P_1 \cup P_2$. Furthermore, we notice that:

$$
\deg((1-p)(1-g_{m+1}p)) = \deg(1-p) + \deg(1-g_{m+1}p) = d_1 + d_2
$$

and that:

$$\deg(p\,(1 - r_{k+1}(1 - p))) = \deg(p) + \deg(1 - r_{k+1}(1 - p)) = d_2 + d_1$$

Finally, we get that:

$$\deg(\pi_3) = \max(\deg((1 - p)(1 - g_{m+1}p)), \deg(p\,(1 - r_{k+1}(1 - p)))) = d_1 + d_2$$

concluding that $P_1, P_2 \vdash^{\mathsf{NS}}_{d_1+d_2} 1$.

$\square$

3 Treelike Res and Nullstellensatz

Definition 4 ($\mathbb{F}_2$-NS encoding of Res)**.** Given a Res linear clause $C = \bigvee_{i=0}^{k_1} x_i \vee \bigvee_{j=0}^{k_2} \overline{x_j}$, the $\mathbb{F}_2$-NS encoding of C is defined as $\mathrm{enc}(C) := \prod_{i=0}^{k_1} x_i \cdot \prod_{j=0}^{k_2}(1 - x_j)$.

In general, a $\mathsf{Res}(\oplus)$ formula $F = C_1 \wedge \ldots \wedge C_m$ defined on the variables $x_1, \ldots, x_n$ gets encoded in $\mathbb{F}_2$-NS as the set of axioms $P_F = \{\mathrm{enc}(C_i) = 0 \mid 1 \leq i \leq m\} \cup \{x_j^2 - x_j = 0 \mid 1 \leq j \leq n\}$.

Theorem 1. *Let F be an unsatisfiable* CNF*. If T is* $\mathsf{Res}(\oplus)$ *refutation of F of size s then there is* NS *refutation of F of degree $O(\log(s))$.*

Proof. Let $F = C_1 \wedge \cdots \wedge C_n$. We proceed by strong induction on the size s.

If $s = 1$ then the T contains only the empty clause $\perp$, meaning that it also is one of the starting clauses and thus one of the axioms. We notice that $\mathrm{enc}(\perp) = 1$, which easily concludes that $\perp \vdash_0^{\mathsf{NS}} 1$.

Suppose now that $s > 1$. Let $\mathcal{L}$ be axioms of T. Since T is a binary tree, by Lemma 1 we know that there is a clause C_k, i.e. a node, of T such that T_{C_k} has size between $\left\lfloor \frac{1}{3}s \right\rfloor$ and $\left\lceil \frac{2}{3}s \right\rceil$.

Let $T' = (T - T_{C_k}) \cup \{C_k\}$. Due to the size of T_{C_k}, we get that T' has size between $\left\lfloor \frac{1}{3}s \right\rfloor + 1$ and $\left\lceil \frac{2}{3}s \right\rceil + 1$. Moreover, we notice that since T is a treelike refutation it holds that T_{C_k} and T' work with different clauses (except C_k), thus their axioms are disjoint. Let $\mathcal{L}_1, \mathcal{L}_2$ be the two sets of axioms respectively used by T_{C_k} and T'.

By construction, we notice that T_{C_k} derives the clause C_k using the axioms $\mathcal{L}_1$, while T_{C_k} derives the clause $\perp$ using the axioms $\mathcal{L}_2, C_k$. Thus, since T_{C_k} and T' have size lower than s, by induction hypothesis we get that $\mathrm{enc}(\mathcal{L}_1) \vdash^{\mathsf{NS}}_{c_1 \cdot \log s} \mathrm{enc}(C_k)$ and $\mathrm{enc}(\mathcal{L}_2), \mathrm{enc}(C_k) \vdash^{\mathsf{NS}}_{c_2 \cdot \log s} 1$ for some constants c_1, c_2. By Proposition 1 we easily conclude that $\mathrm{enc}(\mathcal{L}_1), (1 - \mathrm{enc}(C_k)) \vdash^{\mathsf{NS}}_{c_1 \cdot \log s} 1$ and, by Lemma 2, that $\mathrm{enc}(\mathcal{L}_1), \mathrm{enc}(\mathcal{L}_2) \vdash^{\mathsf{NS}}_{(c_1 + c_2) \cdot \log s} 1$. Finally, since $\mathcal{L}_1 \cup \mathcal{L}_2 = \mathcal{L}$, we get that $\mathrm{enc}(\mathcal{L}) \vdash^{\mathsf{NS}}_{(c_1 + c_2) \cdot \log s} 1$, meaning that $\mathcal{L}$ has a NS refutation of degree $O(\log s)$.

$\square$

4 Treelike $\mathsf{Res}(\oplus)$ and Nullstellensatz

Definition 5 ($\mathbb{F}_2$-NS encoding of Res)**.** Given a $\mathsf{Res}(\oplus)$ linear clause $C = \bigvee_{i=0}^{k}(\ell_i = \alpha_i)$, the $\mathbb{F}_2$-NS encoding of C is defined as $\mathrm{enc}_{\oplus}(C) := \prod_{i=0}^{k}(\alpha - \ell_i)$.
In general, a $\mathsf{Res}(\oplus)$ formula $F = C_1 \wedge \ldots \wedge C_m$ defined on the variables $x_1, \ldots, x_n$ gets encoded in $\mathbb{F}_2$-NS as the set of axioms $P_F = \{\mathrm{enc}_{\oplus}(C_i) = 0 \mid 1 \leq i \leq m\} \cup \{x_j^2 - x_j = 0 \mid 1 \leq j \leq n\}$.

Theorem 2 ([IS20])**.**

1. *Every tree-like* $\mathsf{Res}(\oplus)$ *proof of an unsatisfiable formula* F *may be translated to a parity decision tree for* F *without increasing the size of the tree.*

2. *Every parity decision tree for an unsatisfiable linear CNF may be translated into a tree-like* $\mathsf{Res}(\oplus)$ *proof and the size of the resulting proof is at most twice the size of the parity decision tree (and where the weakening is applied only to the axioms).*

Corollary 1. *Every tree-like* $\mathsf{Res}(\oplus)$ *proof of an unsatisfiable formula* F *can be converted to a tree-like* $\mathsf{Res}(\oplus)$ *proof of at most double the size and with weakening applied only to the axioms.*

Idea: l'idea che mi è venuta per risolvere il problema del weakening che accennavo nell'email parte da un presupposto molto semplice. Siccome per definizione del weakening sappiamo che $C \vdash D$ se $C \implies D$, ciò non implica anche che in NS valga che $\mathrm{enc}_{\oplus}(C) \vdash^{\mathsf{NS}} \mathrm{enc}_{\oplus}(D)$? Se ciò fosse vero, cosa che in teoria possiamo stabilire anche solo per induzione su un albero di size 2 composto solo da queste due clausole (immagino andrebbe dimostrato il caso base), avremmo risolto il problema visto che a quel punto potremmo rimpiazzare ogni clausola weakened con l'assioma che la deriva:

1. Sia $\widehat{C_i}$ il weakening dell'assioma C_i

2. Per induzione dimostriamo che $\mathrm{enc}_{\oplus}(\widehat{C_1}), \ldots, \mathrm{enc}_{\oplus}(\widehat{C_n}) \vdash^{\mathsf{NS}}_{c \cdot \log s} 1$. Questo ci implica che il grado di ogni traduzione dei weakening debba avere degree $\leq c \cdot \log s$

3. Se $\mathrm{enc}_{\oplus}(C_i) \vdash^{\mathsf{NS}} \mathrm{enc}_{\oplus}(\widehat{C}_i)$ allora ciò è possibile solo se $\mathrm{enc}_{\oplus}(C_i) \vdash^{\mathsf{NS}}_{c \cdot \log s}$ $\mathrm{enc}_{\oplus}(\widehat{C}_i)$ visto che altrimenti avremmo che $\deg(\mathrm{enc}_{\oplus}(\widehat{C}_i)) > c \cdot \log s$.

4. Per Proposition 1 vale che $\mathrm{enc}_{\oplus}(C_i), (1 - \mathrm{enc}_{\oplus}(\widehat{C}_i)) \vdash^{\mathsf{NS}}_{c \cdot \log s} 1$

5. Per il Lemma 2 vale che $\mathrm{enc}_{\oplus}(C_1), \mathrm{enc}_{\oplus}(\widehat{C_2}), \ldots, \mathrm{enc}_{\oplus}(\widehat{C_n}) \vdash^{\mathsf{NS}}_{c \cdot \log s} 1$

6. Ripetendo per ogni weakening otteniamo che $\mathrm{enc}_{\oplus}(F) \vdash^{\mathsf{NS}}_{c \cdot \log s} 1$.

L'unico punto critico di questa idea sarebbe dunque stabilire che $\mathrm{enc}_{\oplus}(C_i) \vdash^{\mathsf{NS}}$ $\mathrm{enc}_{\oplus}(\widehat{C}_i)$ valga effettivamente. Sinceramente credo valga anche solo perche intuitivamente si tratta di trovare un polinomio che moltiplicato a $\mathrm{enc}_{\oplus}(C_i)$ generi qualcosa che "contiene" $\mathrm{enc}_{\oplus}(C_i)$, ma ovviamente non è detto che l'intuizione sia effettivamente vera.

5 Bibliography

References

[DMN+21] Susanna F. De Rezende, Or Meir, Jakob Nordström, et al. "Nullstellensatz Size-Degree Trade-offs from Reversible Pebbling". In: *Comput. Complex.* 30.1 (June 2021). ISSN: 1016-3328. DOI: 10.1007/s00037-020-00201-y. URL: https://doi.org/10.1007/s00037-020-00201-y.

[IS20] Dmitry Itsykson and Dmitry Sokolov. "Resolution over linear equations modulo two". In: *Annals of Pure and Applied Logic* 171.1 (2020), p. 102722. ISSN: 0168-0072. DOI: https://doi.org/10.1016/j.apal.2019.102722. URL: https://www.sciencedirect.com/science/article/pii/S0168007219300855.

[LSH65] P. M. Lewis, R. E. Stearns, and J. Hartmanis. "Memory bounds for recognition of context-free and context-sensitive languages". In: *6th Annual Symposium on Switching Circuit Theory and Logical Design (SWCT 1965)*. 1965, pp. 191–202. DOI: 10.1109/FOCS.1965.14.