# Homogenization and the Polynomial Calculus


Josh Buresh-Oppenheim*
Computer Science Department
University of Arizona
Tucson, AZ 85721
Fax: 1-520-621-4246
bureshop@cs.arizona.edu

Matt Clegg
Computer Science and Engineering
University of California, San Diego
La Jolla, CA
mclegg@okbridge.com

Russell Impagliazzo†
Computer Science and Engineering
University of California, San Diego
La Jolla, CA
russell@cs.ucsd.edu

Toniann Pitassi‡
Computer Science Department
University of Arizona
Tucson, AZ 85721
toni@cs.arizona.edu


November 13, 2000


**Abstract**

In standard implementations of the Gröbner basis algorithm, the original polynomials are homogenized so that each term in a given polynomial has the same degree. In this paper, we study the effect of homogenization on the proof complexity of refutations of polynomials derived from Boolean formulas in both the Polynomial Calculus (PC) and Nullstellensatz systems. We show that the PC refutations of homogenized formulas give crucial information about the complexity of the original formulas. The minimum PC refutation degree of homogenized formulas is equal to the Nullstellensatz refutation degree of the original formulas, whereas the size of the homogenized PC refutation is equal to the size of the PC refutation for the originals. Using this relationship, we prove nearly linear ($\Omega(n/logn)$ vs. $O(1)$) separations between Nullstellensatz and PC degree, for a family explicitly constructed contradictory 3CNF formulas. Previously, a $\Omega(n^{1/2})$ separation had been proved for equations that did not correspond to any CNF formulas, and a $\log n$ separation for equations derived from kCNF formulas.



**Keywords:** proof complexity, algebraic proofs, groebner basis algorithm, satisfiability.



*Research partially supported by NSF grant CCR-9457782 and a scholarship from the Arizona Chapter of the ARCS Foundation.

†Research supported by NSF CCR-9734911, Sloan Research Fellowship BR-3311, and by a cooperative research grant INT-9600919/ME-103 from NSF and the MŠMT (Czech Republic), and USA-Israel-BSF Grant 97-00188

‡ Research supported by NSF grant CCR-9457782 and US-Israel BSF Grant 95-00238.

# 1 Introduction

Buchberger's algorithm is a very popular technique from algebraic geometry, which is used to find a Gröbner basis for a family of polynomial equations over variables $x_1,\ldots,x_n$.

Buchberger's algorithm can be applied to solve SAT. Starting with an initial boolean formula in conjunctive normal form, $C = C_1 \wedge C_2 \wedge \ldots \wedge C_m$, convert each clause $C_i$ into an equivalent polynomial equation (over some field $F$), and add the additional equations $x_i^2 - x_i = 0$ to force 0/1 solutions. The corresponding family of polynomial equations will have a solution over $F$ if and only if $C$ is satisfiable. Conversely, $C$ is unsatisfiable if and only if 1 is in the ideal generated by these polynomials, and hence is in the Gröbner basis.

Buchberger's algorithm has many unspecified aspects, such as a term order, and the order in which $S$-remainders are computed. Any specification of these parameters yields a valid Gröbner basis algorithm, but the running time can vary highly depending on these issues. Many heuristics and modifications have been suggested and implemented to make the algorithm simpler or faster. However, typically the algorithm is applied in the context of infinite fields, and thus the heuristics commonly considered may be meaningless or counter-productive in our setting. We are interested in understanding which heuristics work well and why in our setting. One basic heuristic is homogenization. The original system of polynomials is replaced by an equivalent system that is homogeneous, i.e., all terms of a polynomial in the system have the same degree. For systems of polynomials derived from Boolean formulas, we show that homogenization basically creates a hybrid between two well-studied proof systems, Nullstellensatz (HN) and Polynomial Calculus (PC).

The Nullstellensatz (HN) and Polynomial Calculus (PC) proof systems, first defined in [BIK$^+$96, CEI96], are algebraic proof systems for refuting systems of unsolvable polynomial equations. They have been extensively studied in the past several years, due to their connections to standard proof systems, [Pit97, BIK$^+$97] and NP-search classes, as well as Buchberger's algorithm. The two common complexity measures for proofs in these systems are degree and size. We show that the *size* of PC proofs is preserved under homogenization. However, the *degree* can increase dramatically. In fact, the degree of PC proofs for the homogenized polynomials is exactly that of HN proofs for the original polynomials. Using this characterization, we are able to derive an almost optimal separation for PC and HN degrees. We give explicit 3-CNF contradictions whose translations have $O(1)$ degree PC proofs, but require $\Omega(n/\log n)$ degree HN proofs. Previously, a $\Omega(n^{1/2})$ separation had been proved for a system of Boolean polynomials that did not correspond to any CNF ([CEI96, Bus97]), and a $\log n$ separation for equations derived from *kCNF* formulas [BP96].

It follows, from the first result, that if our term order uses only the degree of the homogenizing variable as a tie-breaker, homogenization is guaranteed not to substantially change the time of Buchberger's algorithm for Satisfiability. However, the second result indicates this might not be the case for degree-respecting term orders, as are used in standard implementations.

# 2 Background

## 2.1 Gröbner bases

The theory of Gröbner bases requires an ordering on the terms of the polynomial ring in which we operate. In this case, we choose an arbitrary ordering on the variables and use any induced order on the terms (such as lex, grlex, etc). We use the following definition and theorem, which are both standard to the theory of Gröbner bases ($deg(f)$ is the degree of $f$, LT is the largest term under the ordering, and LCM is the least common multiple):

DEFINITION 2.1: A finite subset $G$ of an ideal $I$ (over a polynomial ring $R$) is called a *Gröbner basis* if it generates $I$, and if the set $\{\mathrm{LT}(g) \mid g \in G\}$ generates the monomial ideal $\mathrm{LT}(I) = \{\mathrm{LT}(f) \mid f \in I\}$.

**Theorem 1:** [CO92] For $G$ a basis for $I$ and $g_1, g_2 \in G$, let

$$S(g,g') = \frac{\mathrm{LCM}(\mathrm{LT}(g),\mathrm{LT}(g'))}{\mathrm{LT}(g)}g - \frac{\mathrm{LCM}(\mathrm{LT}(g),\mathrm{LT}(g'))}{\mathrm{LT}(g')}g'.$$

$G$ is a Gröbner basis for $I$ if and only if for all $g, g' \in G$, there exist $\{a_f\}_{f\in G} \subset R$, such that

$$S(g,g') = \sum_{f\in G} a_f f$$

and $\deg(a_f f) \leq \deg(S(g,g'))$ for all $f \in G$.

$S(g,g')$ is called the S-polynomial of $g$ and $g'$. The S-remainder, written $S(g,g') \mod G$, is the remainder of $S(g,g')$ divided by (the elements of) $G$ (listed in some fixed order). Informally the above theorem states that if $G$ is a basis for $I$, then $G$ is Gröbner if and only if, for all $g, g' \in G$, the S-remainder of $g$ and $g'$ is zero. This theorem gives rise to the following algorithm, commonly called Buchberger's algorithm, for constructing a Gröbner basis. The input to the algorithm is a set of polynomials $F = (f_1, \ldots, f_s)$. Initially, the basis (called $G$) contains $F$. At each step, we select a pair of polynomials in $G$, compute their S-remainder and, if it is non-zero, we add it to $G$. The algorithm terminates when all pairs of polynomials in $G$ have $S$-remainders of zero.

This algorithm is a cornerstone of computational algebraic geometry. Many heuristics have been invented and analyzed for improving the runtime. However, in most applications, the algorithm is applied to infinite fields, and thus it is not clear whether these heuristics make sense in our setting, where the underlying field is finite and solutions are 0/1 valued.

We also mention a well-known lemma for computing $S$-remainders:

**Lemma 2:** [CO92] Let $g$ and $g'$ be two polynomials such that

$$\gcd(\mathrm{LT}(g),\mathrm{LT}(g')) = 1.$$

The S-remainder of $g$ and $g'$ is 0.

## 2.2 Homogeneous Gröbner Bases

Let $F$ be a finite set of polynomials. Let $I_F$ be the ideal generated by $F$, and let $I_F(d)$ be the subset of the ideal consisting of all those polynomials in $I_F$ of degree at most $d$. For solving instances of SAT, we are interested in knowing whether or not $I_F(0)$ is empty.

It is natural to consider a truncated version of the Gröbner basis algorithm where we ignore all S-polynomials of degree greater than $d$. We will let $[d] - \mathit{Grobner}(F)$ denote the output of this truncated version of the algorithm applied to $F$. It would be nice if $[d] - \mathit{Grobner}(F)$ had all of the nice properties of a Gröbner basis for those polynomials in $I_F(d)$. In particular, we would like the largest terms of $[d] - \mathit{Grobner}(F)$ to generate the largest terms of $I_F(d)$. However, in general this is not the case since S-remainders of high degree can lead to new basis elements of very low degree.

On the other hand, the truncated Gröbner basis algorithm does have this nice property when applied to *homogeneous* polynomials. For our purposes, a polynomial $P$ is *homogeneous* if every term in $P$ has the same degree. If every polynomial in $F$ is homogeneous, it can easily be seen that all non-zero S-polynomials will also be homogeneous, and all polynomials output by the Gröbner basis algorithm will be homogeneous. Moreover, to test a particular polynomial $f$ for membership in $I_F$, it suffices to compute $[d]-Grobner(F)$, where $deg(f) = d$.

Because of this and other nice properties, common implementations of the Gröbner basis algorithm begin by homogenizing $F$, if it is not already homogeneous. To do this, a new variable $Z$ is introduced, that is last in the variable ordering. Before running the algorithm, each initial equation $f_i \in F$ is modified (by multiplying each term by a power of $Z$) so that each term in $f_i$ has degree equal to $deg(f_i)$.

The trade-off ensues from the fact that, in the homogenized setting, the polynomials in the ideal may have higher degree than their corresponding polynomials in the non-homogenized setting (i.e. there could be extra factors of $Z$ increasing their degree. We will see that, while a non-homogenized PC-proof consists of testing for elements in $I_F(0)$, we must check for membership of $Z^c$, for some *a priori* unknown constant $c$, to prove the homogenized case.) In this paper we analyze the complexity of the homogenized versus non-homogenized approach, applied to equations derived from 3CNF formulas.

### 2.3 Algebraic Proof Systems

In this paper, we consider two particular algebraic proof systems (i.e. systems under which clauses of an unsatisfiable logical formula are translated into algebraic equations which are then proven to be contradictory). The first is the Hilbert Nullstellensatz (HN) system and the second, the Polynomial Calculus (PC) system. Both rely on the fact that given a contradictory set of polynomials, $Q_1,\ldots,Q_m \in K[X]$ for some field $K$, those polynomials generate the unit ideal in the ring $K[X]$. In other words, the equations do not have a solution in the algebraic closure of $K$ if and only if 1 is in the ideal generated by $Q_i(\overline{x})$. There are several ways of characterizing the elements of this ideal in terms of linear combinations of the generators. Such a demonstration that 1 is in the ideal is thus a *proof* of the unsolvability of the equations $Q_i$. The Nullstellensatz and Polynomial Calculus systems are based on two such characterizations. The standard versions of both assume the variables are Boolean, that is, they take $x^2 - x$ as axiomatic. However, the homogenizing variable will not be Boolean, so we need to consider the extensions of these systems to non-Boolean systems.

Under HN, a proof or refutation is given by exhibiting a sum, $\sum_{i=1}^m P_i Q_i = 1$, for any $\{P_i\}_{i=1}^m \subset K[X]$. The degree of this derivation, then, is $\max\{\deg(P_i Q_i) \mid 1 \le i \le m\}$. Its size is $\sum_{i=1}^m \text{size}(P_i)$ where $\text{size}(P_i)$ is the number of monomials in the polynomial $P_i$. The HN degree of a set of contradictory polynomials is the degree of the minimum-degree HN proof.

A PC derivation of $Q \in K[X]$ from $Q_1,\ldots,Q_n \in K[X]$ is a sequence of polynomials $P_1,\ldots,P_m = Q$, where each $P_i$ is either

1. $Q_j$ for some $j$.
2. $mP_j$ for $j < i$ and $m$ a term in $K[X]$.
3. $aP_j + bP_l$ for $j,l < i$ and $a,b \in K$.

The size of this derivation is $l$. Its degree is $\max\{\deg(P_i) \mid 1 \le i \le l\}$. The PC degree of $Q$ from a set of polynomials is the degree of the minimum-degree PC derivation of $Q$ from those polynomials. If no such derivation exists (i.e. $Q \notin \langle Q_1,\ldots,Q_m\rangle$), then the PC degree of $Q$ is $\infty$. A PC proof or refutation of a set of contradictory polynomials is a PC derivation of 1 from those polynomials. A PC refutation of a set of contradictory polynomials homogenized by $Z$ is a PC derivation of $Z^c$ for any integer $c \geq 0$. The PC degree of a set of contradictory, non-homogenized polynomials is the degree of the minimum-degree proof of those polynomials. The PC degree of a set of contradictory, homogenized polynomials is the minimum over all $c$ of the PC degree of $Z^c$ from those polynomials. Notice that, since a PC proof allows cancellation of terms at each step, its degree is always at most the HN-degree for the same set of polynomials.

## 3 Relationships between complexity measures

The following theorem shows that the homogenized PC degree and the HN-degree are basically the same.

**Theorem 3:** Let $\{q_1, \ldots, q_m\} \subset K[x_1, \ldots, x_n]$. Let $\{Q_1, \ldots, Q_m\} \subset K[X_1, \ldots, X_n, Z]$ be the homogenizations of the above polynomials. Then, $Z^k \in \langle Q_1, \ldots, Q_m \rangle$ iff $\{q_1, \ldots, q_m\}$ has a degree $k$ Hilbert Nullstellensatz (HN) refutation.

**Proof:** First assume $\{q_1, \ldots, q_m\}$ has a degree $k$ HN refutation: $f = \Sigma p_i q_i = 1$, for some $\{p_1, \ldots, p_m\} \subset K[x_1, \ldots, x_n]$ such that $\max \deg(p_i q_i) = k$. Let $f_\alpha$ be the terms of $f$ with multidegree $\alpha = (d_1, \ldots, d_n)$ and $\Sigma d_i = d$. Clearly $f_\alpha = 0$ for all non-trivial $\alpha$. Now let $F = \Sigma Z^{k-\deg(pq)} P_i Q_i$, where $P_i$ is the homogenization of $p_i$. Now, the terms of $f_\alpha$ have become the terms of multidegree $\alpha' = (d_1, \ldots, d_n, k-d)$. Thus, for non-trivial $\alpha$, $F_{\alpha'} = 0$. For $\alpha = 0$, $f_\alpha = 1$, so $F_{\alpha'} = Z^k$. Hence, $F = Z^k$.

Now assume $Z^k \in \langle Q_1, \ldots, Q_m \rangle$. Then we have $\Sigma p_i Q_i = Z^k$ for some $\{p_1, \ldots, p_m\} \subset K[X_1, \ldots, X_n, Z]$. But we can remove all the terms from $p_i$ such that $\deg(p_i Q_i) \geq k$ since they must all cancel. Let's say this yields $p'_i$. Then we set $Z = 1$ on both sides of the equation, so we have $\Sigma(p'_i|_{Z=1}) q_i = 1$ where each term in the sum has degree $k$. Hence $\{q_1, \ldots, q_m\}$ has a degree $k$ HN refutation. □

**Corollary 4:** The degree of the Polynomial Calculus (PC) refutation for $\{Q_1, \ldots, Q_m\}$ is equal to the degree of the HN refutation for $\{q_1, \ldots, q_m\}$.

**Proof:** A PC refutation for $\{Q_1, \ldots, Q_m\}$ consists of deriving $Z^k$ for some $k$. Clearly the degree of this derivation must be at least $k$. But by the theorem, there is a degree $k$ HN refutation of $\{q_1, \ldots, q_m\}$, so $\deg_{PC}(Q_1, \ldots, Q_m) \geq \deg_{HN}(q_1, \ldots, q_m)$. On the other hand, if there is a degree $k$ HN refutation of $\{q_1, \ldots, q_m\}$, then $\{Q_1, \ldots, Q_m\}$ derive $Z^k$ and we saw in the above proof that this can be done in degree $k$, so $\deg_{PC}(Q_1, \ldots, Q_m) \leq \deg_{HN}(q_1, \ldots, q_m)$. □

The following theorem, proven in [BIK$^+$97] shows that the degree of tree-like PC refutations is very close to the degree of HN refutations.

**Theorem 5:** If there is a degree $d$ HN refutation of $Q$, then there is a tree-like, degree $d$ PC refutation of $Q$. Conversely, if there is a tree-like, degree $d$, size $S$ PC refutation of $Q$, then there is a HN refutation of $Q$ of degree $O(d \log S)$.

Lastly, we show that the size of a homogenized PC refutation is no larger than the size of a PC refutation.

**Theorem 6:** Let $q = \{q_1, \ldots, q_m\}$ be a family of polynomial equations and let $Q = \{Q_1, \ldots, Q_m\}$ be the homogenizations of the above polynomials. If $q$ has a size $s$ PC refutation, then $Q$ has a size $O(s)$ homogenized PC refutation.

**Proof:** Let $P$ be a PC refutation of $q$. We will show by induction on the number of lines in $P$, $|P|$, that for all polynomials $r$, if there exists a size $s$ proof of $r$ from $q$, then there exists an $i$ and a size $O(s)$ proof of $RZ^i$ from $Q$, where $R$ is the homogenization of $r$. For the base case, suppose that $r$ has a one line proof from $q$. Then $r$ is an equation of $q$, so $R$ is an initial equation of $Q$ and we are done. Assume the inductive hypothesis holds for $l$ lines, and now let $r$ have an $l+1$-line proof from $q$. There are two cases to consider. The first case is where $r = xt$, where $t$ has an $l$-line proof from $q$. In this case, by induction there exists $i$ such that $TZ^i$ has a small proof from $Q$. But then $R = TZ^i x$ is a proof from $Q$ and we are done. The other case is when $r = r_1 + r_2$, where $r_1$ and $r_2$ each have short proofs from $q$. Without loss of generality, suppose that $deg(r_1) = deg(r_2) + c$. Then $R = R_1 + R_2 Z^c$. By induction, there exist $i$, $j$ such that there are small proofs of $R_1 Z^i$, and $R_2 Z^j$ from $Q$. If $j = c + i$, we have $(R_1 - R_2 Z^c) Z^i$ and we are done. Otherwise, if $j > c + i$, multiply $R_1 Z^i$ by $Z^\delta$ where $\delta = j - c - i$. Then we have $(R_1 - R_2 Z^c) Z^{i+\delta}$. Finally, if $j < c + i$, let $\delta = c + i - j$ and multiply $R_2 Z^j$ by $Z^\delta$ and get $(R_1 - R_2 Z^c) Z^i$. $\square$

# 4 Lower bound for HN-degree

## 4.1 Formulas on graphs

The idea behind these unsatisfiable formulas first appeared in [RM97], and has also appeared in subsequent papers [BEGJ98, BSW99]. We begin with a directed, acyclic graph, $D$, where each node has constant indegree. This graph is viewed as a general implication graph as follows: (1) there is one variable, $X(v)$, corresponding to each vertex $v$ in the graph; (2) for each vertex $v$ in $S$, the set of sources, the corresponding variable $X(v)$ is true; (3) for each non-source vertex $v$ with parent vertices $P(v)$, we have that if all of the variables corresponding to vertices in $P(v)$ are true, then $X(v)$ is also true; (4) finally, to make the formula false, for some sink vertex $t$, $X(t)$ is false.

Throughout this section, we will assume there is only one sink (if not, identify all the sinks to one node). Also, we will abuse notation and use $v$ for $X(v)$. The meaning should be clear from the context. Formally, we define the following clauses: for any $v \notin S$, we have the implication $\bigwedge_{u \in P(v)} u \to v$. Also, we have the axioms $s$ for each $s \in S$. Finally, we insist on $\bar{t}$. If the indegree of $D$ is $k$, then the above formula is a $k+1$-CNF formula.

For algebraic proof systems, we fix a field $K$ and convert the above implications into equations in the ring $K[X(V)]$ (we use the notation $\mathrm{prod}(U)$ to mean $\prod_{u \in U} X(u)$ for $U$ a set of nodes):

$$v\,\mathrm{prod}(P(v)) - \mathrm{prod}(P(v)) = 0.$$

We also include equations restricting the variables to boolean values: $v^2 - v = 0$. Again, if the indegree of $D$ is $k$, then these equations have degree $k+1$.

The natural way to refute the above formula/equations is to begin at the source vertices, and derive successively that each layer of vertices must be true, until finally we can conclude that each sink vertex must be true. This gives us the desired contradiction since there is some sink vertex that is false. For any graph $D$ with indegree $k$, this natural refutation can be formalized as a PC refutation of degree $k+1$, and also as a polynomial-size tree-like Resolution refutation. However, we show here that if the graph is sufficiently complicated (it has high pebbling number), then any HN refutation must have high degree.

Our lower bound strategy will be to take advantage of Corollary 4. That is, we will implicitly describe a Gröbner basis for the above equations, and then prove that the degree of this basis is at least as large as the pebbling number associated with the underlying graph.

### 4.2 Gröbner basis for graph formulas

Consider the homogenized implications and restrictions (for each $v$):

$$v\,\text{prod}(P(v)) - Z\,\text{prod}(P(v)) = 0, \qquad v^2 - vZ = 0.$$

Here $Z$ is the variable added for homogenization. We also have the assertions (for each source $s$):

$$s - Z = 0,$$

which will be considered implications saying that the empty set implies $s$, and (for one sink $t$):

$$t = 0.$$

Let $I$ be the ideal generated by these equations. In practise, the proof of our lower bound is focused on implications. Hence, instead of deriving $Z^d$ (for some $d$), we simply try to derive the equation

$$f = (t\,\text{prod}(S) - Z\,\text{prod}(S))Z^d.$$

To see that this works and is still a proof, assume that we have derived $Z^d$. Then clearly we can derive $f$ (or any other multiple of $Z^d$). On the other hand, if we have derived $f$ then

$$-f + (Z-t)(\sum_{i=1}^{|S|}(s_i - Z)\prod_{j=i+1}^{|S|} s_j) + t = Z^{d+|S|+1}.$$

Although we have derived a higher power of $Z$ than we assumed, the proof remains valid. As for the degree of the proof, we use the concept of *Z-degree*:

DEFINITION 4.1: Let $P \in K[X,Z]$ be a homogenized polynomial. We define the *Z-degree* of $P$, $\text{zdeg}(P)$ to be the maximal $m \in \mathbf{N}$ such that $P/Z^m \in K[X,Z]$.

The Z-degree of $f$, then, is $d$ and we shall consider this the *de facto* degree of the proof. Notice that a lower bound for $\text{zdeg}(f)$ is a lower bound for the power of $Z$ which we can derive and hence is a lower bound on the HN-degree.

Now we are ready to explore the Gröbner basis for our ideal. We first exhibit certain polynomials in the ideal:

**Proposition 7:** Let $V_1, V_2 \subset V$, $u_1, u_2 \in V$, $d_1, d_2 \geq 0$ and assume that the implications

$$f_1 = (u_1\,\text{prod}(V_1) - Z\,\text{prod}(V_1))Z^{d_1}, \qquad f_2 = (u_2\,\text{prod}(V_2) - Z\,\text{prod}(V_2))Z^{d_2}$$

are in $I$. If $u_1 \in V_2$, then let $U = V_1 \cup V_2 - \{u_1\}$ and let $d = \max\{d_1, d_2\}$. We can then conclude that $(u_2\,\text{prod}(U) - Z\,\text{prod}(U))Z^{d+1}$ is in $I$.

**Proof:**

$$\begin{aligned}(Z^{d-d_2}\,\text{prod}(V_1 - V_2))f_2 - (u_2 - Z)(Z^{d-d_1}\,\text{prod}(V_2 - V_1 - \{u_1\}))f_1 \\ = (u_2\,\text{prod}(U) - Z\,\text{prod}(U))Z^{d+1}.\end{aligned}$$

□

Let $V \to u$ denote the formula stating that if all of the variables in $V$ are true, then $u$ is also true. Informally the above proposition says that if we have a degree $d_1$ PC derivation of $V_1 \to u_1$, and a degree $d_2$ PC derivation of $V_2 \to u_2$, where $u_1 \in V_2$, then we can derive $V_1 \cup V_2 - \{u_1\} \to u_2$ in degree $max(d_1, d_2) + 1$ (notice that this is still true for the degenerate case where $V_1 = \emptyset$). See figures 1 and 2 for a graphical representation. Let $G$ be the set of equations formed recursively as follows:

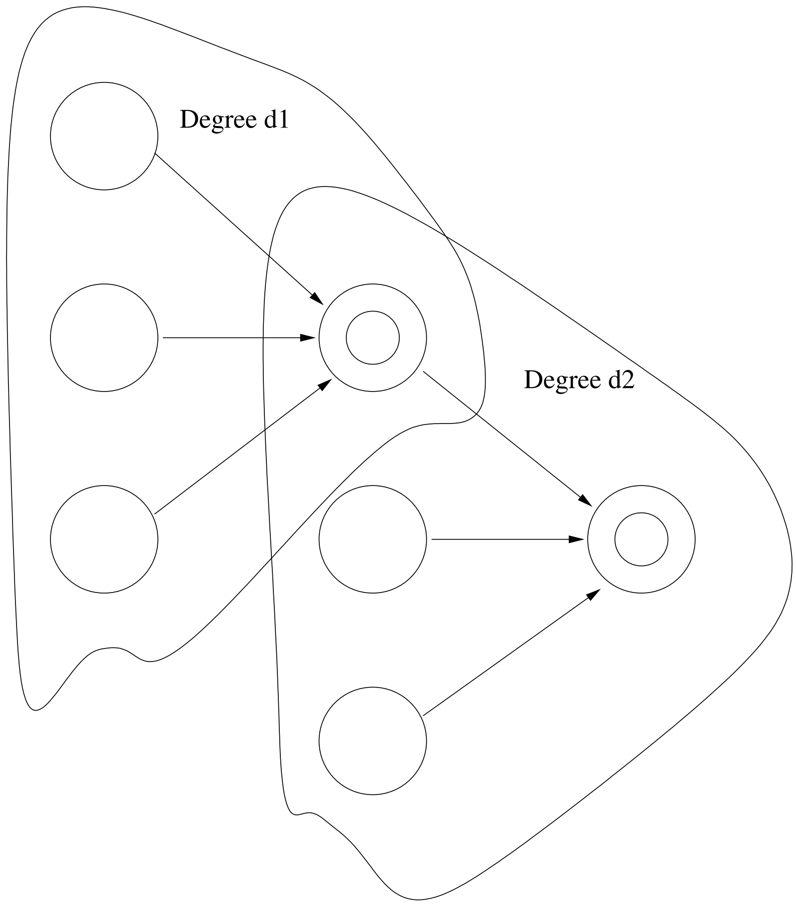


Figure 1: Two implications where the conclusion of one is included in the hypothesis of the other.

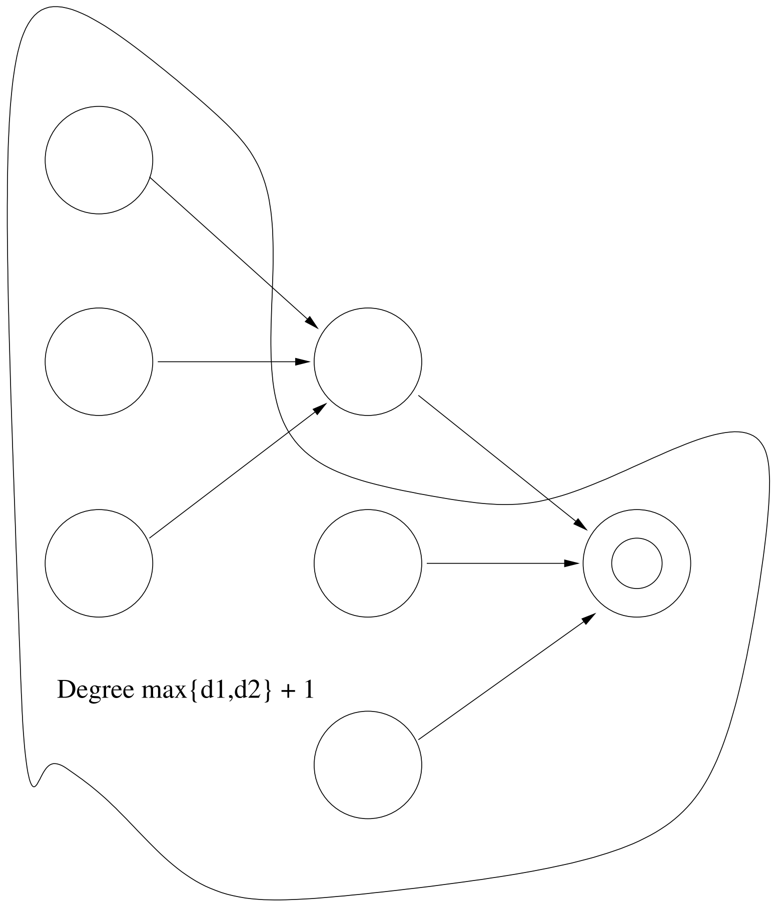


Figure 2: The implication derived from the previous two.

1. $G$ contains all of the generators of $I$.
2. If the implications

$$f_1 = (u_1 \operatorname{prod}(V_1) - Z \operatorname{prod}(V_1))Z^{d_1}, \qquad f_2 = (u_2 \operatorname{prod}(V_2) - Z \operatorname{prod}(V_2))Z^{d_2}$$

   are in $G$ and $u_1 \in V_2$, then

$$(u_2 \operatorname{prod}(U) - Z \operatorname{prod}(U))Z^{d+1}$$

   is in $G$.

$G$, then, is just the closure under applications of Proposition 7. It is not hard to see that, invariably, the conclusion node of each implication is not included among the hypothesis nodes, since the hypothesis nodes are all predecessors of the conclusion node and the graph is acyclic. We shall use this fact in proving that $G$ is a very fundamental set:

**Theorem 8:** $G$ is a Gröbner basis for $I$.

**Proof:** Clearly $G$ is a basis since it contains all of the generators of $I$. We show that it is Gröbner using Theorem 1 (recall that we defined $Z$ to be last in the ordering of the variables). Consider two implications,

$$f_1 = (u_1 \operatorname{prod}(V_1) - Z \operatorname{prod}(V_1))Z^{d_1},$$
$$f_2 = (u_2 \operatorname{prod}(V_2) - Z \operatorname{prod}(V_2))Z^{d_2}.$$

The S-remainder is

$$S(f_1, f_2) = (\operatorname{prod}(V_1 \cup V_2 \cup \{u_2\} - \{u_1\})Z - \operatorname{prod}(V_2 \cup V_1 \cup \{u_1\} - \{u_2\})Z)Z^d.$$

Here and throughout, we omit any cases of two polynomials with relatively prime largest terms by Lemma 2. Hence there are three remaining possibilities for implications:

1. $u_1 = u_2$: If $u_1 = u_2$, then the S-remainder becomes

$$(\operatorname{prod}(V_1 \cup V_2)Z - \operatorname{prod}(V_1 \cup V_2)Z)Z^d.$$

   But the two terms are clearly equal, so the S-remainder is 0.

2. $u_1 \in V_2$: Recall from above that $u_2 \notin V_1$ since $V_1$ consists of predecessors of $u_1$, $u_1$ is a predecessor of $u_2$ and the graph is acyclic. Consider the first term of the S-remainder:

$$t_1 = \operatorname{prod}(V_1 \cup V_2 \cup \{u_2\} - \{u_1\})Z^{d+1}.$$

   But we know that

$$g = (u_2 \operatorname{prod}(V_1 \cup V_2 - \{u_1\}) - Z \operatorname{prod}(V_1 \cup V_2 - \{u_1\}))Z^{d+1}$$

   is in $G$ by definition. So $t_1$ can be reduced to a lower-degree term:

$$t_1 - g = \operatorname{prod}(V_1 \cup V_2 - \{u_1\})Z^{d+2}.$$

   The second term is $t_2 = \operatorname{prod}(V_2 \cup V_1 \cup \{u_1\} - \{u_2\})Z^{d+1}$. Since $u_2 \notin V_1$, this is the same as $\operatorname{prod}(V_2 \cup V_1 \cup \{u_1\})Z^{d+1}$. Also, we have $f_1 \in G$, so we can reduce the second term:

$$t_2 - \operatorname{prod}(V_2 - (V_1 \cup \{u_1\}))Z^{d-d_1+1} f_1 = \operatorname{prod}(V_1 \cup V_2 - \{u_1\})Z^{d+2}.$$

   These two expressions are the same, so we have reduced $S(f_1, f_2)$ to 0.

3. $u_1 \neq u_2$, $u_1 \notin V_2$ and $u_2 \notin V_1$, but $V_1 \cap V_2 \neq \emptyset$: Now, the S-remainder is

$$(\operatorname{prod}(V_1 \cup V_2 \cup \{u_2\})Z - \operatorname{prod}(V_1 \cup V_2 \cup \{u_1\})Z)Z^d.$$

   Let $t_1$ be the first term and $t_2$ be the second. Then,

$$t_1 - \operatorname{prod}(V_1 - V_2)Z^{d+1-d_2} f_2 = \operatorname{prod}(V_1 \cup V_2)Z^{d+2}.$$

   Similarly,

$$t_2 - \operatorname{prod}(V_2 - V_1)Z^{d+1-d_1} f_1 = \operatorname{prod}(V_1 \cup V_2)Z^{d+2}.$$

   Again, we have reduced the S-remainder to 0.

This concludes the S-remainders for every pair of implications in $G$. We now consider the S-remainders involving the boolean restrictions. Let $h = u^2 - uZ$. Then,

$$S(h_1, f_2) = \operatorname{prod}(V_2 \cup \{u_2\} - \{u\})uZ^{d_2+1} - u \operatorname{prod}(\{u\} - \{u_2\} - V_2) \operatorname{prod}(V_2)Z^{d_2+1}.$$

Again we have cases:

1. $u = u_2$: We can then assume that $u \notin V_2$, so the S-remainder becomes

$$u \operatorname{prod}(V_2)Z^{d_2+1} - u \operatorname{prod}(V_2)Z^{d_2+1} = 0.$$

2. $u \in V_2$ and $u \neq u_2$: In this case, the S-remainder is

$$\operatorname{prod}(V_2 \cup \{u_2\})Z^{d_2+1} - u \operatorname{prod}(V_2)Z^{d_2+1}.$$

   If we call the first term $t_1$ and the second $t_2$, consider $t_1 - Zf_2 = \operatorname{prod}(V_2)Z^{d_2+2}$. We can rewrite $t_2$ as $u^2 \operatorname{prod}(V_2 - \{u\})Z^{d_2+1}$. But then $t_2 - \operatorname{prod}(V_2 - \{u\})Z^{d_2+1}h_1 = u \operatorname{prod}(V_2 - \{u\})Z^{d_2+2}$. But this is just $\operatorname{prod}(V_2)Z^{d_2+2}$ so we are done.

Finally, we have the odd case of the equation $t = 0$.

1. Consider $h_1$, where $u = t$. $S(h_1, t) = tZ$, but $t$ is in $G$, so it reduces to 0.
2. Similarly, we have $f_1$, where $u_1 = t$. $S(f_1, t) = tZ^{d_1+1}$, so again it reduces to 0.

We have now shown that all the S-remainders are 0 modulo $G$ and can conclude (by Theorem 1) that $G$ is Gröbner . □

### 4.3 Lower bound for induction principle

We will now use the above characterization of the basis to prove degree bounds for various graphs. First, we will prove a lower bound on the HN-degree of an important formula that defines the induction principle. Consider the graph $(\{u_i\}_{i=1}^n, \{(u_i, u_{i+1})\}_{i=1}^{n-1})$ (see figure 3).

It represents the "induction" principle, which [BP96] have shown by other methods to have HN-degree $\Theta(\log n)$. Here we show the result using the Gröbner basis.

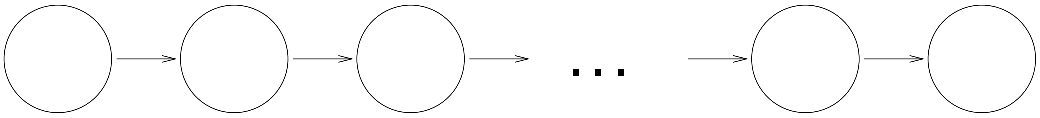

Figure 3: The induction principle

**Proposition 9:** If the equation $g = (u_1 u_n - u_1 Z)Z^c$ is in the Gröbner basis for the formula on the above graph, then $c \geq \lceil \log n \rceil$.

**Proof:** We prove the claim by induction. Assume for $1 \leq i < j \leq n$ and $j - i < n$, that if $(u_i u_j - u_i Z)Z^{c'} \in G$, then $c' \geq \lceil \log(j-i) \rceil$. We know from the Gröbner basis that $g$ must have been generated by two equations: namely, $(u_1 u_l - u_1 Z)Z^{d_1}$ and $(u_l u_n - u_l Z)Z^{d_2}$, where $1 < l < n$ and $c = \max\{d_1, d_2\} + 1$. But, $\max\{l-1, n-l\} \geq \lceil n/2 \rceil$, so $\max\{d_1, d_2\} \geq \lceil \log(n/2) \rceil$. It follows that $c \geq \lceil \log n \rceil$. □

**Theorem 10:** [BP96] The formula has HN-degree $\Omega(\log n)$.

**Proof:** Let $g = (u_1 u_n - u_1 Z)Z^c$ where $c$ is the minimal exponent such that $g$ is in the Gröbner basis. From the proposition, we know that $c \geq \lceil \log n \rceil$. But the equations in $G$ with largest term $u_1 u_n Z^d$ for some power $d$ are all simply multiples of $g$ by $Z^{d-c}$. Since the largest terms of the Gröbner basis generate the largest terms of the ideal, any equation $f = (u_1 u_n - u_1 Z)Z^e$ that can be derived, must have $e \geq c$. □

### 4.4 Near-optimal lower bounds and Pebbling

Strong lower bounds for specific graphs will easily follow by showing that any HN derivation can easily be converted into an efficient pebbling strategy for the corresponding graph. Interesting connections between pebbling and propositional proofs were made previously in [ET99, BSW99].

DEFINITION 4.2: Let $D = (V, E)$ be a directed, acyclic graph. A configuration is a subset of $V$. A legal pebbling of a vertex $v$ in $D$ is a sequence of configurations, the first being the empty set and the last being $\{v\}$ and in which each configuration $C'$ follows from the previous configuration $C$ by one of the following rules:

1. $v$ can be added to $C$ to get $C'$ if all immediate predecessors of $v$ are in $C$.
2. Any vertex can be removed from $C$ to obtain $C'$.

The *complexity* of a legal pebbling of $v$ is the maximal size of any configuration in the sequence. The *pebbling number of a graph D* with a single sink vertex $s$ is the minimal number $n$ such that there exists a legal pebbling of $s$ with complexity $n$.

**Lemma 11:** Let $D$ be a directed, acyclic graph, and let $Q_D$ be the corresponding unsatisfiable system of homogeneous equations corresponding to the implication formula associated with $D$. If $Q_D$ has a degree $d$ PC refutation, then $D$ has pebbling complexity $O(d)$.

**Proof:** In Theorem 8, we gave a recursive characterization of the polynomials in the Grobner basis. We'll show by induction on the depth of a polynomial in this recursion, that if $(u\,\mathrm{prod}(U) - Z\,\mathrm{prod}(U))Z^d$

is in the Groebner basis, then $u$ can be pebbled from $U$ with $d+k$ pebbles. The base case is the axioms $v\,\mathrm{prod}(P(v)) - Z\,\mathrm{prod}(P(v))$, which can always be pebbled with $k$ pebbles (if $k$ is the maximum in-degree of $D$). Otherwise, $(u\,\mathrm{prod}(U) - Z\mathrm{prod}(U))Z^d$, was derived from $(v\,\mathrm{prod}(V_1) - Z\,\mathrm{prod}(V_1))Z_1^d$, and $(u\,\mathrm{prod}(V_2) - Z\,\mathrm{prod}(V_2))Z_2^d$, where $d = \max d_1, d_2+1$, $v \in V_2$, $v \notin V_1$ and $U = V_1 \cup V_2 - \{v\}$; these formulas having been already derived. Thus, by the induction assumption, we can pebble $v$ from $V_1$ with $d_1+k$ pebbles and $u$ from $V_2$ with $d_2+k$ pebbles. Then we can pebble $u$ from $U$ as follows. First, pebble $v$ from $V_1 \subseteq U$. Then, leaving a pebble on $v$, pebble $u$ from $V_2 \subseteq U \cup \{v\}$. The number of pebbles is at most the larger of $d_1+k$ and $d_2+k+1$, which is at most $d+k$. □

We note that the above lemma is not tight, as can be seen with the linear graph corresponding to the induction principle. In this case, the pebbling number is 2, whereas the degree is $\log n$. We do, however, get the following result:

**Theorem 12:** There is a directed acyclic graph with constant in-degree that requires HN degree $\Omega(n/logn)$.

**Proof:** [CPT77] exhibits a graph based on a construction by Valiant that has $n$ nodes and in-degree 2, but has pebbling measure $\Omega(n/logn)$. By the lemma, we are done. □

## 5 Comparison with Resolution

The PC system gives rise to Buchberger's algorithm to solve SAT as mentioned above. The HN system gives rise to a simpler algorithm for SAT whereby one solves a system of *linear* equations. That is, if we start with a system of equations $Q$ (including $x^2 - x = 0$ for all variables $x$), and we assume they have a degree $d$ HN proof, then it can be found as follows. Consider an alleged degree $d$ proof, $\sum_i P_i Q_i = 1$, where the polynomials $P_i$ are indeterminants, represented by vectors of variables, $x_i^t$, where $x_i^t$ represents the coefficient in front of term $t$ in the polynomial $P_i$. Solving for the $P_i$'s amounts to solving a sparse system of linear equations (in the variables $x_i^t$), where we have one equation for each term of degree at most $d$. This algorithm has runtime $n^{O(d)}$, and hence is efficient if $d$ is small. [CEI96] gives comparable upper bounds for this algorithm and Buchberger's algorithm.

Complete algorithms for SAT with the best empirical performance are Resolution based, and typically are variations on the Davis-Loveland-Logeman (DLL) procedure. Here we show that with respect to worst-case complexity, the algorithms are incomparable.

**Lemma 13:** The graph formulas mentioned above (with maximum pebbling number) have polynomial-size Tree-like Resolution (DLL) proofs but require nearly linear degree HN proofs.

**Proof:** To see that the graph formulas always have small Tree-like Resolution proofs, simply order the vertices of the graph in such a way that if $v$ is a vertex with parents $P(v)$, then all vertices in $P(v)$ appear before $v$ in the ordering. Then a tree-like Resolution proof can be constructed as a decision tree, where we query the vertices according to the ordering described above. The height of the tree will be equal to the number of vertices, but the width will be constant. □

**Lemma 14:** The Tseitin graph principles (mod $p$) have constant degree HN proofs in the field $GF_p$ but require exponential-size Resolution proofs.

**Proof:** [Urq87] has shown that the Tseitin graph principles require exponential-size Resolution proofs. To see that they have polynomial-size HN proofs, consider the clauses that correspond to a particular vertex, expressing that the number of edges incident to that vertex is odd. Each such clause converts into an initial equation, and the set of equations assocated with a vertex $v$ can be used to derive the equation stating that the sum of the vertices incident to that vertex is 1 mod 2. Since the total number of variables mentioned in these equations is constant, the HN degree of this derivation is constant. Do this for every vertex, and then simply add up the resulting equations to derive $1 = 0$. $\square$

## 6 Acknowledgments

We would like to thank Will Evans for very helpful conversations.

## References

[BEGJ98] M.L. Bonet, J. L. Esteban, N. Galesi, and J. Johannsen. Exponential separations between restricted resolution and cutting planes proof systems. In *Proceedings from 38th FOCS*, pages 638–647. 1998.

[BIK+96] Paul W. Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.*, 73(3):1–26, 1996.

[BIK+97] S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computation Complexity*, 6(3):256–298, 1997.

[BP96] S. R. Buss and T. Pitassi. Good degree bounds on Nullstellensatz refutations of the induction principle. In *Proceedings of the Eleventh Annual Conference on Computational Complexity (formerly: Structure in Complexity Theory)*, pages 233–242, Philadelphia, PA, May 1996. IEEE.

[BSW99] E. Ben Sasson and A. Wigderson. Short proofs are narrow–resolution made simple. In *Proceedings of 31st ACM STOC*, pages 517–526. 1999.

[Bus97] S. R. Buss. Lower bounds on Nullstellensatz proofs via designs. In P. W. Beame and S. R. Buss, editors, *Proof Complexity and Feasible Arithmetics*, DIMACS, pages 59–71. American Math. Soc, 1997.

[CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Gröbner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 174–183, Philadelphia, PA, May 1996.

[CO92] J. Cox, D. Little and D. O'Shea. *Ideals, Varieties and Algoirthms*. Springer-Verlag, 1992.

[CPT77] R. Celoni, W.J. Paul, and R.E. Tarjan. Space bounds for a game on graphs. *Math. Systems Theory*, 10:239–251, 1977.

[ET99] J. L. Esteban and Jacobo Toran. Space bounds for resolution. In *Proc. 16th STACS*, pages 551–561. Springer-Verlag LNCS, 1999.

[Pit97] T. Pitassi. Algebraic propositional proof systems. In *DIMACS Series in Discrete Mathematics*, volume 31, pages 215–243. American Math. Soc, 1997.

[RM97] R. Raz and P. McKenzie. Separation of the monotone nc hierarchy. In *Proceedings of 38th IEEE Foundations of Computer Science*. 1997.

[Urq87] A. Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, 1987.