On first-order theorem proving using generalized odd-superpositions II*

WU Jinzhao (吴尽昭)

(Department of Mathematics, Peking University, Beijing 100871, China)

and LIU Zhuojun (刘卓军)

(Institute of Systems Science, Chinese Academy of Sciences, Beijing 100080, China)

Received June 24, 1996

Abstract It is shown that the proof system using odd-superpositions II is not complete. The reason leading to this incompleteness is that the use of idempotency rule is neglected. By defining the superpositions of first-order polynomials and zero, the concept of odd-superpositions II is extended, and a complete proof system using the extended odd-superpositions II is developed. In addition, this proof system is an improvement on remainder method; its completeness demonstrates actually that the remainder method using semantic strategy is still complete.

Keywords: theorem proving, first-order polynomials, odd-superpositions II, generalized odd-superpositions II, odd factors.

The proof system developed in ref. [1] is important both theoretically and practically. Its inference rule is the computation of odd-superpositions and odd-factors. Similar to resolution principle, we know that it is useful to define the superpositions of two arbitrary first-order polynomials. We can thus, for example, consider introducing not only semantic strategy as ref. [1] did, but also lock strategy and linear strategy[2]. This is very significant because lock strategy is well known to be efficient, and we can easily apply various tree searching techniques if linear strategy is employed. However, the odd-superposition computation is not symmetric in some way. If we want to similarly define a superposition of any two first-order polynomials, and guarantee the completeness of the proof system, such a superposition has to consist of two first-order polynomials in general. This is like NC-resolution[3] and generalized resolution[4, 5]. Therefore, in the proof procedure, more first-order polynomials may be produced. But for odd-superpositions II, such problems do not exist. On the other hand, Wu's method[6] provided us with some techniques of using single overlaps and parallel overlaps, which are superior to multiple overlaps and sequential overlaps[7]. Obviously, it is worth applying the frame of Wu's method to first-order theorem proving. In doing so, we have to adopt a similar computation of odd-superpositions II. We need the concept of the remainders[8] of one first-order polynomial

* Project supported by the Chinese Climbing Project Foundation and China Postdoctoral Science Foundation.
with respect to another one. Roughly speaking, such a remainder is just an odd-superposition II of these two first-order polynomials if substitutions are neglected.

It is an open problem in first-order theorem proving whether the proof system using odd-superpositions II is complete\(^8\). We have defined a concept of remainders which is similar to that of odd-superpositions II when we investigate the application of Wu’s method to first-order theorem proving\(^9\). In this paper, we show that this proof system is not complete. Nevertheless, by introducing a generalized definition of odd-superpositions II, we prove that the proof system with this kind of odd-superposition II as inference rule is complete. Thus this sort of generalization is necessary and appropriate especially for non-clausal theorem proving. However, for clausal theorem proving, we need no such generalization, since in this case odd-superposition II is just the same as odd-superposition. At the same time, our proof system is also an improvement on remainder method\(^8\) which keeps complete. These are the main contents in secs. 2 and 4; in sec. 1, we give some basic concepts and results which our discussions are heavily based on; in sec. 4, we have some related remarks, to discuss the use of simplification rule, etc.

1 Basic concepts and results

For the concepts which are not defined in this paper, the reader may consult references [2, 10].

A first-order polynomial is a polynomial over the ring of residue classes modulo \(2\) with atoms as indeterminates. A first-order polynomial is called ground if the atoms in it are ground. We still call the variables in atoms variables. A product of some non-zero atoms is called a monomial. In the following, we always use \(a, b, c, d, e, r, \cdots\) to represent first-order polynomials, \(m, n, \cdots\) to denote atoms. By \(\bar{c}\) we denote the first-order polynomial obtained by reducing \(c\) by \(BR\). We say that \(c\) is odd, if the number of the monomials in \(\bar{c}\) is odd. Let \(\theta\) be a substitution. \(\bar{c}\theta\) is called an instance of \(c\). If two or more atoms in \(c\) have a most general unifier (mgu for short) \(\sigma\), we call \(\bar{c}\sigma\) a factor of \(c\). In particular, \(\bar{c}\) is also a factor of \(c\). Clearly, the instances of \(c\) are instances of \(\bar{c}\).

For an arbitrary (first-order) formula \(\varphi\), by \(s\varphi\) we denote a Skolem standard form of \(\varphi\). We call the first-order polynomial \(ps\varphi\) defined below the one associated with \(\varphi\):

\[
ps\varphi = \begin{cases} 
    s\varphi, & \text{if } s\varphi \text{ is an atom;} \\
    1 + ps\varphi, & \text{if } s\varphi = \neg \varphi; \\
    (ps\varphi)(ps\varphi), & \text{if } s\varphi = \varphi_1 \land \varphi_2; \\
    \frac{ps\varphi + ps\varphi + (ps\varphi)(ps\varphi)}{ps\varphi + ps\varphi + (ps\varphi)(ps\varphi)}, & \text{if } s\varphi = \varphi_1 \lor \varphi_2; \\
    1 + ps\varphi, & \text{if } s\varphi = \varphi_1 \rightarrow \varphi_2; \\
    1 + ps\varphi, & \text{if } s\varphi = \varphi_1 \leftarrow \varphi_2. 
\end{cases}
\]
where \( \varphi, \varphi_1, \varphi_2 \) are formulae.

We remark that the first-order polynomials associated with \( 1(\text{true}) \) and 0 (false) are defined as 1 and 0, respectively.

Suppose \( F=\{\varphi_1, \ldots, \varphi_n\} \) is a given formula set, and \( PS=\{ps\varphi_1+1, \ldots, ps\varphi_n+1\} \). Then it is sufficient for us to consider if the first-order polynomial set \( PS \) is unsatisfiable.

For a formula \( \varphi \), if \( s\varphi \) is a clause, we call \( ps\varphi+1 \) a clausal first-order polynomial. Thus, \( c \) is clausal if and only if \( c \) is either zero or 1 or of the form \((m_i+c_i)\ldots(m_i+c_i)\), where \( m_i \) are different atoms and \( i \in \{0, 1\} \). Therefore, the instances of (odd) clausal first-order polynomials are still (odd) clausal ones.

Assume that \( H_j \) is the \( j \)-level constants of \( PS \), and \( PS|H_j \) is the set constructed from \( PS \) by replacing each variable in the atoms in each first-order polynomial of \( PS \) by all the elements of \( H_j \) and reduced by BR. Then we have

**Lemma 1.1 (Herbrand Theorem)**\(^9\). \( F \) is unsatisfiable if and only if there is a \( j \in \{0, 1, \ldots\} \), such that \( PS|H_j \) is unsatisfiable.

In the following, \( >_p \) is a partial ordering (a transitive and irreflexive binary relation) on atoms, and \( m >_p l >_p 0 \) holds for any \( m \). \( >_p \) is called stable if for any \( m, n \) and any substitution \( \theta \), \( m >_p n \) implies \( m\theta >_p n\theta \). We say that \( m \) is maximal (minimal) in an atom set \( A \), if for any \( n \in A \), \( n >_p m \) (\( m >_p n \)).

In this paper, all the atoms mentioned are neither 0 nor 1 unless otherwise specified. We always suppose that \( PS \) is the first-order polynomial set defined above, and \( >_p \) is stable. We use \( A \) to denote the set of all the atoms in \( \bar{c} \). \( A, \theta = \{m\theta|m \in A\} \), where \( \theta \) is a substitution. Sometimes a first-order polynomial in which the powers of all the atoms are one is directly written in the form \( am + b \), where \( m \notin A \).

**2 Proof system**

We first show that the proof system using odd-superpositions II is not complete. Then, we modify the definition of odd-superpositions II, and describe a proof system with the modified odd-superpositions II as inference rule. We will consider the completeness of our proof system in the next section.

**2.1 A problem**

There is an open problem: Is the proof system with the computation of odd-superpositions II and odd-factors as inference rule complete\(^{13, 30}\)? Unfortunately, we have the following counter-examples:

**Example 2.1.1.** \( PS = \{c_1 = f(x)g(x) + g(x)h(x) + h(x)f(x), c_2 = g(c) + 1, c_3 = h(c) + 1\} \).
Theorem 2.1.1. The proof system with the computation of odd-superpositions II and odd-factors as inference rule is not complete.

However, for clausal first-order polynomial sets, since odd-superposition II is the same as odd-superposition and N-superposition\(^\text{11}\), we have

Theorem 2.1.2. For clausal first-order polynomial sets, the proof system with the computation of odd-superpositions II and odd-factors as inference rule is complete.

Since non-clausal theorem proving has obvious advantages over clausal theorem proving\(^\text{11, 13, 4}\), we want to pay more attention to non-clausal theorem proving.

2.2 The proof system using generalized odd-superpositions II

The reason for the incompleteness is that the computation of odd-superpositions II cannot offer all necessary information derived from the idempotency rule \(B_2\). So we must find out such information. We can give a solution by defining superpositions of first-order polynomials and zero, where the zero represents in fact the idempotency rule \(B_2\).

Let \(c_i = a_i m_1 + b_i\) and \(a_i m_2 + b_2\) be a factor of \(c_i\). Suppose \(\sigma\) is an mgu of \(m_1\) and \(m_2\). We call \((a_i b_1 + a_i b_2)\sigma\) a superposition of \(c_1\) and \(c_2\) upon \(m_1\sigma\), and \(b_i(a_i + b_i)\) a superposition of \(c_i\) and \(0\) (upon \(m_i\)). If \(\sigma\) is the empty substitution, sometimes we also call \((a_i b_1 + a_i b_2)\sigma\) a superposition of \(c_1\) and \(c_2\) upon \(m_i\). Similarly, we sometimes call \(b_i(a_i + b_i)\) a superposition of \(c_i\) and \(0\) upon \(m_i\sigma\), where \(\sigma\) can be considered as the empty substitution.

By the definition of remainders\(^\text{19}\), we have

Theorem 2.2.1. The superpositions of \(c_1\) and \(c_2\) are remainders of \(c_1\) and \(c_2\).
Our proof system uses the computation of generalized odd-superpositions II and odd-factors defined in the following as inference rule.

\[ \text{c} \text{c} \sigma \] is called an odd-factor of c, if (a) c is odd; (b) \( \sigma \) is an mgu of \( m, n, n \in A \); (c) \( m \sigma \) is maximal in \( A, \sigma \). Obviously, \( \overline{cc} \sigma \) is odd.

Suppose \( c_1, \cdots, c_q, c_{q+1} \) are given. For \( p=1 \), let \( r_{q+1} = c_{q+1} \), \( r_q \) be a superposition of \( c_q, r_{q+1} \) upon \( m_q \sigma \). If (a) \( c_1, \cdots, c_q \) are odd; (b) \( m_q \sigma \) is maximal in \( A, \sigma \) for \( p \in \{1, \cdots, q\} \); (c) \( r_q \) is odd, then we call \( c_q, \cdots, c_q, c_{q+1} \) an odd-clash, and \( r_q \) a generalized odd-superposition II of it.

Because \( (a,b_1+a_2,b_2) \sigma = (a,(a,m_1+b_2)) \sigma + (a,(a,m_1+b_2)) \sigma + b_1(a_1+b_2)(a_1+b_2) + a_1(m_1+m_1) \sigma \), the computation of odd-superpositions is sound. Thus, the computation of generalized odd-superpositions II is sound.

We do not have to define the superpositions of a first-order polynomial and zero for clausal theorem proving. As a matter of fact, since clausal first-order polynomials are of special expressions (see sec. 1), we have

**Theorem 2.2.2.** Suppose \( c_1, c_0 \) are clausal. Then (1) any superpositions of \( c_1 \) and \( c_0 \) are still clausal; (2) any superpositions of \( c_1 \) and zero are zero.

3 Completeenss of the proof system

Without loss of generality, we suppose \( PS \) contains a zero. A sequence \( c_1, \cdots, c_k \) is called an odd-deduction from \( PS \) to \( c_k \) if for arbitrary \( t=1, \cdots, k \), either \( c_t \in PS \), or \( c_t \) is an odd-factor of a first-order polynomial before it, or \( c_t \) is a generalized odd-superposition II of an odd-clash constructed by some first-order polynomials before it.

Therefore, if we can show that \( PS \) is unsatisfiable if and only if there exists an odd-deduction from \( PS \) to 1, then we have proved that the proof system with the computation of generalized odd-superpositions \( \Pi \) and odd-factors as inference rule is complete. The “if” part, namely the soundness of the proof system, is obvious, because the computation of generalized odd-superpositions II is sound. To show the “only if” part, following the general technique to construct a deduction sequence to prove the completeness, we divide it into two steps.

3.i The ground case

In this subsection, by \( m \) we denote a ground atom, and \( c(m \downarrow 1) \) the first-order polynomial obtained from \( c \) by replacing \( m \) by 1. Then \( c \) is odd if and only if \( c(m \downarrow 1) \) is odd.

**Lemma 3.1.1.** If \( \overline{a} \neq 0 \), then \( a+b+ab \neq 0 \).
Using mathematical induction on the number of the elements of $A_n$, we can prove this conclusion easily.

**Lemma 3.1.2.** Suppose $c_1$ and $c_2$ are ground, $\overline{c_i}(m \leftarrow 1) \neq 0$. Let $n$ be ground, and $r$ the superposition of $c_1(m \leftarrow 1)$ and $c_2(m \leftarrow 1)$ upon $n$. If $\overline{c_i}(m \leftarrow 1) \neq 0$, let $r$ be the superposition of $c_1$ and $c_2$ upon $n$; otherwise, let $r$ be the superposition of $c_1$ and zero upon $n$. Then $r(m \leftarrow 1) = r'$.

**Proof.** Let $\overline{c_i} = (a(m + 1) + b) n + e_i(m + 1) + d_i$, where $m, n \notin A_{a_i} \cup A_{b_i} \cup A_{e_i} \cup A_{d_i}$ ($j = 1, 2$). Then $\overline{c_i}(m \leftarrow 1) = b_i n + d_i$. By the definition of superpositions, we can obtain $r(m \leftarrow 1) = r'$.

**Q.E.D.**

**Lemma 3.1.3.** Let $c = a(m + 1) + 1$, $\overline{a} \neq 0$, $m \notin A_n$, and let $m$ be minimal in $A_n$. Then there exists an odd-deduction from $\{c, 0\}$ to $m$.

**Proof.** $c$ is obviously odd. Using mathematical induction on the number of the elements of $A_n$, and by Lemma 3.1.1, we can get the result as required.

**Q.E.D.**

**Lemma 3.1.4.** Suppose $c_1, c_2$ are ground, $m, n \notin A_{c_1}, m, n \notin A_{c_2}, m \notin A_{c_1(m \leftarrow 1)}$, but $m \notin A_{c_2(m \leftarrow 1)}$. Let $r$ be the superposition of $c_1$ and $c_2$ upon $m$, let $r_1$ be the superposition of $c_1$ and zero upon $m$, and let $r_2$ be the superposition of $r_1$ and $c_2$ upon $m$. Then, $r(m \leftarrow 1) = r_2(m \leftarrow 1)$.

**Proof.** Suppose $\overline{c_i} = (a(m + 1) + b) m + e_i(m + 1) + d_i$, $m, n \notin A_{c_1} \cup A_{c_2} \cup A_e \cup A_d$. Since $m \notin A_{c_1(m \leftarrow 1)}$, $m, n \notin A_{c_2(m \leftarrow 1)}$, we have

$$a(m \leftarrow 1) = 0, b(m \leftarrow 1) = 0, c(m \leftarrow 1) \neq 0.$$ 

We can also compute $r_i = (cm_i + d)(am_i + cm_i + b + d) = (ac + bc + ad + c) m_i + bd_i + d_i$. In addition,

$$m_i \in A_{c_i(m \leftarrow 1)} \text{ (in fact, } r_i(m \leftarrow 1) = \overline{c_i}(m \leftarrow 1)), m_i \in A_{c_i},$$

because $(ac + bc + ad + c)(m \leftarrow 1) = c(m \leftarrow 1) \neq 0$.

Thus, in the two cases of $\overline{c_i} = 0$ and $m_i \in A_{c_1}$, $r_2(m \leftarrow 1) = r(m \leftarrow 1)$.

**Q.E.D.**

We remark that in the above three lemmas, if $m$ is replaced by $0$, the conclusions also hold.

**Theorem 3.1.1.** Suppose PS is a ground first-order polynomial set. If PS is unsatisfiable, then there exists an odd-deduction from PS to 1.

**Proof.** By refining $>_p$ on ground atoms, we can assume that the generalized odd-superpositions II of an odd-clash constructed by ground first-order polynomials are unique. Now we want to prove the theorem by using mathematical induction on the number $l$ of the elements in $\bigcup_{c \in PS} A_c$. 

If \( l = 0 \), there exists \( c \in PS \), such that \( c = 1 \). Therefore \( c \) is an odd-deduction from \( PS \) to 1.

Suppose that the theorem holds for \( l < h \). For \( l = h \), two cases should be considered.

Case 1. There is an odd \( c_n \in PS \) such that \( A_n \) contains only one atom.

Suppose \( c_n = m \). Let \( PS' = \{ c(m \cdot 0) | c \in PS \} \), where \( c(m \cdot 0) \) represents the first-order polynomial obtained from \( c \) by replacing \( m \) by 0. Then \( PS' \) is unsatisfiable, and the number of the elements of \( \bigcup \{ m \in PS : A \} \) is less than \( h \). By the induction hypothesis, there exists an odd-deduction \( D' \) from \( PS' \) to 1. For any \( c'_i \) in \( D' \), if there exists \( c_i \in PS \), such that \( c'_i = c_i(m \cdot 0) \) (we choose \( c_i = 0 \) if \( c'_i = 0 \)), then keep \( D' \) invariant if \( c'_i = c_i \); otherwise, add \( c_n \), \( c_i \) to \( D' \) and put them before \( c_i \). It \( c'_i \) is the generalized odd-superposition II of an odd-clash before it in \( D' \), keep \( D' \) invariant.

Suppose that we eventually get a first-order polynomial sequence \( D \) by dealing with \( D' \) above. It is not hard to see that \( c_n \), \( c_i \) is an odd-clash if \( c'_i \) is odd, and its generalized odd-superposition II is \( c'_i \). If \( c'_i \) is not odd, suppose \( c'_i, \ldots, c'_q \), \( c'_i \) is an odd-clash in \( D' \), and \( c'_i \) is the generalized odd-superposition II of it. If \( c'_i \notin c_i \), then \( c'_i, \ldots, c'_i, c_i \) is an odd-clash, and \( c'_i \) is the generalized odd-superposition II of it. So \( D \) is an odd-deduction from \( PS \) to 1.

Case 2. There is no \( c_n \in PS \) such that \( c_n \) is odd and \( A_n \) contains only one atom.

Let \( m \) be a minimal atom in \( \bigcup \{ m \in PS : A \} \). \( PS' = \{ c(m \cdot 1) | c \in PS \} \). Similarly we know \( PS' \) is unsatisfiable and the number of the elements of \( \bigcup \{ m \in PS : A \} \) is less than \( h \). By the induction hypothesis, there exists an odd-deduction \( D' = c'_1, \ldots, c'_k \) (\( c'_i = 1, k \geq 1 \)) from \( PS' \) to 1. For an arbitrary \( c'_i \) in \( D' \), if there is \( c_i \in PS \), such that \( c'_i = c_i(m \cdot 1) \) (we choose \( c_i = 0 \) if \( c'_i = 0 \)), then replace \( c'_i \) by \( c_i \) in \( D' \). Otherwise, let \( c'_i \) be the generalized odd-superposition II of an odd-clash \( c'_1, \ldots, c'_q \), \( c'_1, c'_1, \ldots, c'_{t(q+1)} \) \( (1, \ldots, t(q+1) < t) \) in \( D' \), and suppose \( r_{q+1}, r_{q+2}, \ldots, r_{t(q+1)} \) are the superposition of \( c'_1, c'_1, \ldots, c'_{t(q+1)} \) upon \( m_p \), \( r'_{q+1}, r'_{q+2}, \ldots, r'_{t(q+1)} \) upon \( m_p \) \( (p = q - 1, \ldots, 1) \), and \( r_{q+1} = c'_i \). Assume in \( D' \): \( c'_1, \ldots, c'_q, c'_1, c'_1, \ldots, c'_{t(q+1)} \) have been replaced by \( c'_1, \ldots, c'_q, c'_1, c'_1, \ldots, c'_{t(q+1)} \) respectively, and \( c'_i = c_i(m \cdot 1) \), \( c'_i = c_i(m \cdot 1) \), \( c'_i = c_i(m \cdot 1) \).

Let \( d_{i(q+1)} = c_{i(q+1)} \). Replace \( c_{i(q+1)} \) by \( d_{i(q+1)} \) in \( D' \).

If \( m_i \) is maximal in \( A_i \), let \( r_{q+1} \) be the superposition of \( c_{i(q+1)} \) upon \( m_i \). By Lemma 3.1.2, we have

\[
r_{q+1}(m \cdot 1) = r_{i(q+1)}.
\]

Otherwise we might as well assume that \( n_i, n_i \in A_{i(q+1)} \), such that \( n_i > m_i \), \( n_i > m_i \), and \( n_i > m_i \).

Since \( n_i \notin A_{i(q+1)} \), we can write \( c_{i(q+1)} \) in the form \( c_{i(q+1)} = a(m_i + 1)n_i + c(m_i + 1) + d \). \( m_i, n_i \notin A_i \cup A_i \cup A_i \). Since \( c_{i(q+1)} = d \), \( d \) is odd. Thus, \( c_{i(q+1)} \) is odd. However, the superposition of \( c_{i(q+1)} \) and
zero upon $n_i$ is

$$v_{q} = \frac{(c(m_q + 1) + d)(a(m_q + 1) + c(m_q + 1) + d)}{\text{odd}}$$

so $v_{q}$ is odd. It also implies $c_{iq}, 0$ is an odd-clash, and $v_{q}$ is the generalized odd-superposition II of it. If $n_{q} \notin A_{q+i}$, let $d_{iq} = v_{iq}$, replace $c_{iq}$ by $d_{iq}$ in $D'$, and add $c_{iq}, 0$ to $D'$, before $d_{iq}$. Obviously, $m_q$ is maximal in $A_{q+i}$. Let the superposition of $d_{iq}$ and $d_{iq+1}$ upon $m_q$ be $r_{iq}$. From Lemmas 3.1.4, 3.1.2, we have

$$r_{iq}(m \leftarrow 1) = r_{iq}'.$$

Otherwise, if $n_{q} \in A_{q+i}$, let $g_{iq}$ be the superposition of $v_{iq}$ and zero upon $n_{q}$. Similarly, we can prove that $v_{iq}, 0$ is an odd-clash, and $g_{iq}$ is the generalized odd-superposition II of it, $m_q$ is maximal in $A_{q+i}$. Now let $d_{iq} = g_{iq}$. In $D'$, replace $c_{iq}$ by $d_{iq}$, and add $c_{iq}, 0, v_{iq}, 0$ to $D'$ before $d_{iq}$. In the same way, if $r_{iq}$ is the superposition of $d_{iq}$ and $d_{iq+1}$ upon $m_q$, then

$$r_{iq}(m \leftarrow 1) = r_{iq}'.$$

Suppose in $D'$, $c_{iq}'$ has been replaced by $d_{jq}(p < j \leq q + 1)$, and $r_{iq}$ is the generalized odd-superposition II of $c_{ip}$ and $r_{iq+1}$ upon $m_q$. Suppose that $c_{ip}$ has been replaced by $d_{ip}$, and $r_{ip}$ is the superposition of $d_{ip}$ and $r_{ip+1}$ upon $m_q$. Then

$$r_{ip}(m \leftarrow 1) = r_{ip}'.$$

Especially

$$r_{iq}(m \leftarrow 1) = r_{iq}' = c_{iq}.'$$

Obviously, $d_{iq}, \cdots, d_{iq+1}$ is an odd-clash, and $r_{iq}$ is the generalized odd-superposition II of it. Use $r_{iq}$ to replace $c_{iq}'$ in $D'$.

Suppose that we eventually get a first-order polynomial sequence $D$ by dealing with $D'$ above. Then $D$ is an odd-deduction from $PS$ to a $c_{iv}$ and

$$c_{iv}(m \leftarrow 1) = 1,$$

i.e. there exists $a$, $m \notin A_{n}$, such that

$$c_{iv} = a(m + 1) + 1.$$ 

If $a = 0$, $D$ is an odd-deduction from $PS$ to 1. Otherwise, by Lemma 3.1.3, there exists an odd-deduction $D_i$ from $\{c_{iv}, 0\}$ to $m$. From Case 1, we know that there exists an odd-deduction $D_i$ from $PS \cup \{m\}$ to 1. Therefore, $D$, $D_i$, $D_i$ is an odd-deduction from $PS$ to 1.

\textbf{Q.E.D.}

\textbf{Example 3.1.1.} See Example 2.1.2.

$PR + R + 1$, $0$, $P$, $PQ + 1$, $1$ is an odd-deduction from $PS$ to 1.
3.2 Lifting the ground case to the general case

Hereinafter, we finish the completeness proof by the following lifting lemma.

**Lemma 3.2.1.** Suppose $c'$ is odd, $c'$ is an instance of $c$, $m' \in A_\lambda$, and $m'$ is maximal in $A_\lambda$. Then there exists $d$ and an odd-deduction from $\{\overline{c}, 0\}$ to $d$, such that $c' = \overline{d\theta}$, and there is a unique $m \in A_\lambda$, $m\theta = m'$ and $m\theta$ is maximal in $A_\theta$, where $\theta$ is a substitution.

**Proof.** Let $c' = \overline{c\lambda}$, where $\lambda$ is a substitution. Since $c'$ is odd, $c$ is odd. Now we use mathematical induction on the number $l$ of the elements of $A_\lambda$ to complete the proof.

For $l = 1$, let $c = n$. Then $m' = nl$. We can choose $d = c$, $m = n$, $\theta = \lambda$. $\overline{c}$ is an odd-deduction from $\{\overline{c}, 0\}$ to $d$.

Suppose that the conclusion holds for $l < h$. Now, we consider the case of $l = h$. Let $M = \{m \in A_\lambda | m\lambda > m'\}$. There are two cases as follows.

**Case 1.** $M = \emptyset$.

Let $M' = \{m \in A_\lambda | m\lambda = m'\}$. If $M'$ contains only one element $n$, we can choose $d = c$, $m = n$, $\theta = \lambda$, and $\overline{c}$ is an odd-deduction from $\{\overline{c}, 0\}$ to $d$. Otherwise choose two different $m_0$, $m_1 \in M'$. Since $m_0\lambda = m_1\lambda = m'$, there exists an mgu $\sigma$ of $m_0$ and $m_1$. Suppose that $\lambda = \sigma \cdot x$. Then $m_0\sigma$ must be maximal in $A_\sigma$. At the same time, we know $c' = \overline{c\lambda} = \overline{c\sigma \cdot x}$, and $c'$ is an instance of $c\sigma$. Therefore, $c\sigma$ is odd, and $c\sigma$ is an odd-factor of $c$. Obviously, the number of the elements of $A_\lambda < h$. By the induction hypothesis, we know that there are a $d$ satisfying the condition required and an odd-deduction $D_i$ from $\{\overline{c\sigma}, 0\}$ to $d$. Thus $\overline{c}$. $D_i$ is an odd-deduction from $\{\overline{c}, 0\}$ to $d$.

**Case 2.** $M \neq \emptyset$.

Let $N = \{m \in A_\lambda | m\lambda$ is maximal in $A_\lambda\}$. Then $N \cap M \neq \emptyset$. Now we choose some $m_0 \in N \cap M$. If for any $m_1 \in A_\lambda - \{m_0\}$, $m_1 \not= m_0\lambda$, then let $\overline{c} = a_0 + b_0$. It is easy to know $\overline{a_0\lambda} = 0$ and $c' = \overline{a_0\lambda}$, since $m_1\lambda > m'$ and $m'$ is maximal in $A_\lambda$. Furthermore, we claim $m_1$ is maximal in $A_\lambda$. Let $c_1 = a_1 + b_1$. Then $c_1\lambda = b_1(a_1\lambda + b_1\lambda) = b_1 = c'$. So $c'$ is still an instance of $c_1$, which also implies $c_1$ is odd. Therefore, $c_1$ is a generalized odd-superposition II of $c$ and zero. Clearly the number of the elements of $A_\lambda < h$. By the induction hypothesis, we know that there exist a $d$ satisfying the condition required and an odd-deduction $D_i$ from $\{\overline{c_1}, 0\}$ to $d$. Thus $\overline{c}$. $D_i$ is an odd-deduction from $\{\overline{c}, 0\}$ to $d$. If there is an $m \in A_\lambda - \{m_0\}$, such that $m\lambda = m_0\lambda$, then let $\sigma$ be an mgu of $m$ and $m_0$. Similar to the above proof, there exist a $d$ satisfying the requirement and an odd-deduction from $\{\overline{c}, 0\}$ to $d$.

Q.E.D.

**Lemma 3.2.2.** If $1$ is an instance of $c$, then there exists an odd-deduction from $\{\overline{c}, 0\}$ to $1$. 

---

This lemma is a corollary of Lemma 3.2.1.

Lemma 3.2.3 (Lifting lemma). Suppose $c_p$ is ground. It is an instance of $c_p$ ($p = 1, \ldots, q+1$), and $c_{1}, \ldots, c_{q}, C_{(q+1)}$ is an odd-clash; $r_{i_{n}}$ is a generalized odd-superposition of it. Then there exist $r_{i_{n}}$ and an odd-deduction from $\{c_{1}, \ldots, c_{q}, \overline{c_{(q+1)}}, 0\}$ to $r_{i_{n}}$, such that $r_{i_{n}}$ is an instance of $r_{i_{n}}$.

Proof. Let $r_{i_{n+1}} = c_{(q+1)}$. Suppose that $r_{i_{n}}$ is the superposition of $c_{p}$ and $r_{i_{n+1}}$ upon $m_{p}$, where $m_{p}$ is maximal in $A_{c_{p}} (p = 1, \ldots, q)$. Let $c_{p} = a_{p}m_{p} + b_{p}$. By Lemma 3.2.1, there are $d_{p} = a_{p}m_{p} + b_{p}$ and an odd-deduction $D_{p}$ from $\{c_{p}, 0\}$ to $d_{p}$, such that $c_{p} = d_{p} \overline{\theta}$, $m_{p} = m_{p} \overline{\theta}$, and for any $n \in A_{a_{p}} \cup A_{b_{p}}$, $n \theta \neq m_{p}$. Clearly $d_{p}$ is odd, and $a_{p} = a_{p} \overline{\theta}$, $b_{p} = b_{p} \overline{\theta}$.

If $r_{i_{n+1}} = 0$, and $r_{i_{n}} = b_{p}(a_{p} + b_{p})$, then since $m_{p} \overline{\theta}$ is maximal in $A_{d_{p}} \overline{\theta}$ and $a_{p} \overline{\theta}$ is stable, $m_{p}$ is maximal in $A_{d_{p}}$. Let $r_{i_{n}} = b_{p}(a_{p} + b_{p})$. Then $b_{p}(a_{p} \overline{\theta} + b_{p}) = (b_{p}(a_{p} + b_{p})) \overline{\theta}$. Thus $r_{i_{n}}$ is an instance of $r_{i_{n}}$.

If $r_{i_{n+1}} \neq 0$, suppose $r_{i_{n+1}} = a_{p}m_{p} + b_{p}$, and $r_{i_{n}} = b_{p} + a_{p} \overline{\theta}$, and $r_{i_{n}} = b_{p} + a_{p} \overline{\theta}$. By renaming the variables, we assume $d_{p}$ and $r_{i_{n+1}}$ have no common variables. We can thus suppose $r_{i_{n+1}} = d_{p} \overline{\theta}$. In addition, we assume $r_{i_{n+1}} = d_{p} \overline{\theta} = b_{p} + a_{p} \overline{\theta}$, and for any $n \in A_{a_{p}} \cup A_{b_{p}}$, $n \theta \neq m_{p} \overline{\theta}$. Otherwise, we can obtain such a first-order polynomial by computing the factors of $r_{i_{n+1}}$. Obviously $a_{p} \overline{\theta} = a_{p} \overline{\theta}$, $b_{p} \overline{\theta} = b_{p} \overline{\theta}$. Let $\sigma$ be an mgu of $m_{p}$ and $n$. Since $m_{p} \overline{\theta}$ is maximal in $A_{d_{p}} \overline{\theta}$, $m_{p} \overline{\theta}$ is maximal in $A_{d_{p}} \overline{\theta}$. Assume $\alpha$ is a substitution such that $\theta = \sigma \overline{\alpha}$. Then $m_{p} \overline{\theta} = m_{p} \overline{\theta} \overline{\alpha}$. Therefore, $m_{p} \overline{\theta} A_{a_{p}, \sigma} \cup A_{b_{p}, \sigma}$. Let $r_{i_{n}} = (a_{p} \overline{\theta} + a_{p} \overline{\theta}) \overline{\sigma}$. Then $r_{i_{n}} = a_{p} \overline{\theta} + a_{p} \overline{\theta}$. Thus $r_{i_{n}}$ is an instance of $r_{i_{n}}$. Especially, $r_{i_{n}}$ is an instance of $r_{i_{n}}$.

Because $r_{i_{n}}$ is odd, $r_{i_{n}}$ is odd. Hence, $d_{p}$, $\ldots$, $d_{q}$, $c_{(q+1)}$ is an odd-clash, and $r_{i_{n}}$ is a generalized odd-superposition of it. $D_{p}$, $\ldots$, $D_{q}$, $c_{(q+1)}$, $r_{i_{n}}$ is an odd-deduction from $\{c_{i_{n}}, \ldots, c_{i_{n}}, \overline{c_{(q+1)}}, 0\}$ to $r_{i_{n}}$. Q.E.D.

By Lemma 1.1, Theorem 3.1.1, Lifting lemma and Lemma 3.2.2, we have

Theorem 3.2.1. If $PS$ is an unsatisfiable first-order polynomial set, then there exists an odd-deduction from $PS$ to 1.

We have thus proved the proof system using generalized odd-superpositions II is complete.

Example 3.2.1. See Example 2.1.1.

$f(x)g(x) + g(x)h(x) + h(x)f(x)$, $0$, $g(x)h(x)$, $g(c) + 1$, $h(c)$, $h(c) + 1$, $1$ is an odd-deduction from $PS$ to 1.

By Theorem 2.2.1 and Theorem 3.2.1, we know that the proof system using generalized odd-superpositions II is an improvement on remainder method which keeps complete.
Similarly to the proof of Theorem 3.2.1, we have

**Theorem 3.2.2.** The remainder method using semantic strategy is complete.

4 Some remarks

(1) The idea of our proof system is, in fact, that of negative resolution. Dually, we can use the idea of positive resolution, and all the conclusions in this paper still hold if odd first-order polynomials are replaced by those with 1 as one of its monomials.

(2) Using the concept of superpositions defined in this paper, we can introduce the strategies which are similar to linear resolution and lock resolution. We will discuss this problem in another paper.

(3) By applying the technique to shrink a semantic tree\[1, 2\], we can show that our proof system is still complete if the simplification rule defined in ref. [1] is introduced. However, we do have an interesting problem: is the proof system still complete, if we remove condition (c) and do not want to compute the factors of \( c_i \) in the definition of generalized odd-superpositions II?

(4) For the two examples in sec. 2, if we select an appropriate partial ordering on atoms, 1 can be derived from \( PS \). So there is a problem, whether there exists a partial ordering on atoms, such that the proof system with the computation of odd-superpositions II and odd-factors defined in ref. [1] as inference rule is complete. This problem may be significant in theoretical sense.

(5) What our proof system uses are single overlaps and parallel overlaps. And we do not need multiple overlaps and sequential overlaps at all. Since in clausal theorem proving, odd-superposition II is the same as odd-superposition, we have also the conclusion: N-superposition without using multiple overlaps is complete. But another problem is not solved yet. Is the proof system complete, if sequential overlaps are employed in the definition of odd-superpositions II?

(6) The superpositions of two first-order polynomials defined in this paper are similar to the pseudo remainders of two polynomials\[9\]. Our future work will investigate whether the idea of Wu's method, (a) computing basic chains; (b) computing characteristic sets; (c) decomposing the zero set, can be applied to first-order theorem proving to obtain a complete method.

(7) Up to now, Ma Bin from Peking University has implemented linear strategy proposed in ref. [9] using *Mathematica*. The implementation of the whole proof system given in this paper is under developing. Since we need the computation of some factors, our proof system maybe produces more first-order polynomials than that in reference [1].
References