ARTICLE IN PRESS YJSCO:1992

Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

# Polynomial reduction and supercongruences

Qing-Hu Hou [a], Yan-Ping Mu [b], Doron Zeilberger [c]

[a] School of Mathematics, Tianjin University, Tianjin 300350, PR China
[b] College of Science, Tianjin University of Technology, Tianjin 300384, PR China
[c] Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA

ARTICLE INFO

*Article history:*
Received 22 July 2019
Accepted 6 November 2019
Available online xxxx

*Keywords:*
Hypergeometric term
Supercongruence
Polynomial reduction

ABSTRACT

Based on a reduction process, we rewrite a hypergeometric term as the sum of the difference of a hypergeometric term and a reduced hypergeometric term (the reduced part, in short). We show that when the initial hypergeometric term has a certain kind of symmetry, the reduced part contains only odd or even powers. As applications, we derived two infinite families of supercongruences.



## 1. Introduction

In recent years, many supercongruences involving combinatorial sequences have been discovered, see for example, Sun (2014) and Osburn et al. (2016). The standard methods for proving these congruences include combinatorial identities (Sun, 2013), finite field hypergeometric series (Ahlgren and Ono, 2000), symbolic computation (Osburn and Schneider, 2009).

We are interested in the following supercongruence conjectured by van Hamme (1997),

$$\sum_{k=0}^{\frac{p-1}{2}}(-1)^k(4k+1)\left(\frac{(1/2)_k}{(1)_k}\right)^3 \equiv (-1)^{\frac{p-1}{2}}p \pmod{p^3},$$

where $p$ is an odd prime and $(a)_k = a(a+1)\cdots(a+k-1)$ is the rising factorial. This congruence was proved by Mortenson (2008), Zudilin (2009) and Long (2011) by different methods. Sun (2012) proved a stronger version for primes $p \geq 5$,

*E-mail addresses:* qh_hou@tju.edu.cn (Q.-H. Hou), yanping.mu@gmail.com (Y.-P. Mu), doronzeil@gmail.com (D. Zeilberger).

https://doi.org/10.1016/j.jsc.2019.11.004
0747-7171/

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

$$\sum_{k=0}^{\frac{p-1}{2}}(-1)^k(4k+1)\left(\frac{(1/2)_k}{(1)_k}\right)^3 \equiv (-1)^{\frac{p-1}{2}}p+p^3E_{p-3} \pmod{p^4},$$

where $E_n$ is the $n$-th Euler number defined by

$$\frac{2}{e^x+e^{-x}}=\sum_{n=0}^{\infty}E_n\frac{x^n}{n!}.$$

A similar congruence was given by van Hamme (1997) for $p\equiv 1 \pmod 4$:

$$\sum_{k=0}^{\frac{p-1}{2}}(4k+1)\left(\frac{(1/2)_k}{(1)_k}\right)^4 \equiv p \pmod{p^3}.$$

Long (2011) showed that in fact the above congruence holds for arbitrary prime $p\geq 5$ modulo $p^4$. Motivated by these two congruences, Guo (2017) proposed the following conjectures (corrected version).

**Conjecture 1.1.**

- *For any odd integer m, there exists an integer $a_m$ such that for any odd prime p and positive integer s,*

$$\sum_{k=0}^{\frac{p^s-1}{2}}(-1)^k(4k+1)^m\left(\frac{(1/2)_k}{(1)_k}\right)^3 \equiv a_m\cdot p^s(-1)^{\frac{(p-1)s}{2}} \pmod{p^{s+2}}. \tag{1.1}$$

- *For any odd integer m, there exists an integer $b_m$ such that for any odd prime $p\geq(m+1)/2$ and positive integer s,*

$$\sum_{k=0}^{\frac{p^s-1}{2}}(4k+1)^m\left(\frac{(1/2)_k}{(1)_k}\right)^4 \equiv b_m\cdot p^s \pmod{p^{s+3}}. \tag{1.2}$$

Liu (2019) and Wang (2018) confirmed the conjectures for $s=1$ and some initial values $m$. Jana and Kalita (2019) and Guo (2019) confirmed (1.1) for $m=3$ and $s\geq 1$. We will prove a stronger version of (1.1) for the case of $s=1$ and arbitrary odd $m$ and a weaker version of (1.2) for the case of $s=1$ and arbitrary odd $m$ by a reduction process.

Recall that a hypergeometric term $t_k$ is a function of $k$ such that $t_{k+1}/t_k$ is a rational function of $k$. Our basic idea is to rewrite the product of a polynomial $f(k)$ in $k$ and a hypergeometric term $t_k$ as

$$f(k)t_k=\Delta_k(g(k)t_k)+h(k)t_k=(g(k+1)t_{k+1}-g(k)t_k)+h(k)t_k,$$

where $g(k),h(k)$ are polynomials in $k$ such that the degree of $h(k)$ is bounded. To this aim, we construct a polynomial $x(k)$ such that $\Delta_k(x(k)t_k)$ equals the product of $t_k$ and a polynomial $u(k)$ and that $f(k)$ and $u(k)$ has the same leading term. Then we have

$$f(k)t_k-\Delta_k(x(k)t_k)=(f(k)-u(k))t_k$$

is the product of $t_k$ and a polynomial of degree less than that of $f(k)$. We call such a reduction process one reduction step. Continuing this reduction process, we finally obtain a polynomial $h(k)$ with bounded degree. We will show that for $t_k=\left(\frac{(1/2)_k}{(1)_k}\right)^r$, $r=3,4$ and an arbitrary polynomial of form $(4k+1)^m$ with $m$ odd, the reduced polynomial $h(k)$ can be taken as $(4k+1)$. This enables us to reduce the congruences (1.1) and (1.2) to the special case of $m=1$, which is known for $s=1$.

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

We notice that Pirastu and Strehl (1995) and Abramov (1975, 1995) gave the minimal decomposition when $t_k$ is a rational function, Abramov and Petkovšek (2001, 2002) gave the minimal decomposition when $t_k$ is a hypergeometric term, and Chen et al. (2015) applied the reduction to give an efficient creative telescoping algorithm. These algorithms concern a general hypergeometric term. While we focus on a kind of special hypergeometric terms so that the reduced part $h(k)t_k$ has a nice form.

The paper is organized as follows. In Section 2, we consider the reduction process for a general hypergeometric term $t_k$. Then in Section 3 we consider those $t_k$ with the property $a(k)$ is a shift of $-b(k)$, where $t_{k+1}/t_k = a(k)/b(k)$. As an application, we prove a stronger version of (1.1) for the case $s = 1$. Finally, we consider the case when $a(k)$ is a shift of $b(k)$, which corresponds to (1.2). In this case, we show that there is a rational number $b_m$ instead of an integer such that (1.2) holds when $s = 1$.

## 2. The difference space and polynomial reduction

Let $K$ be a field of characteristic zero and $K[k]$ be the ring of polynomials in $k$ with coefficients in $K$. Let $t_k$ be a hypergeometric term. Suppose that

$$\frac{t_{k+1}}{t_k} = \frac{a(k)}{b(k)},$$

where $a(k), b(k) \in K[k]$. It is straightforward to verify that

$$\Delta_k \left(b(k-1)x(k)t_k\right) = (a(k)x(k+1) - b(k-1)x(k))t_k. \tag{2.1}$$

We thus define the *difference space* corresponding to $a(k)$ and $b(k)$ to be

$$S_{a,b} = \{a(k)x(k+1) - b(k-1)x(k) \colon x(k) \in K[k]\}.$$

We see that for $f(k) \in S_{a,b}$, we have $f(k)t_k = \Delta_k(p(k)t_k)$ for a certain polynomial $p(k) \in K[k]$.

Let $\mathbb{N}, \mathbb{Z}$ denote the set of nonnegative integers and the set of integers, respectively. Given $a(k), b(k) \in K[k]$, we denote

$$u(k) = a(k) - b(k-1), \tag{2.2}$$
$$d = \max\{\deg u(k), \deg a(k) - 1\} \tag{2.3}$$

and for $a(k) \neq 0$,

$$m_0 = -\operatorname{lc} u(k)/\operatorname{lc} a(k), \tag{2.4}$$

where $\operatorname{lc} p(k)$ denotes the leading coefficient of $p(k)$. Here we define $\deg 0 = -\infty$ and $\operatorname{lc} 0 = 0$ for convenience.

We first introduce the concept of degeneration.

**Definition 2.1.** Let $a(k), b(k) \in K[k]$ with $a(k) \neq 0$ and let $u(k), m_0$ be given by (2.2) and (2.4). If

$$\deg u(k) = \deg a(k) - 1 \quad \text{and} \quad m_0 \in \mathbb{N},$$

we say that the pair $(a(k), b(k))$ is *degenerated*.

We will see that the degeneration is closely related to the degrees of the elements in $S_{a,b}$.

**Lemma 2.2.** *Let $a(k), b(k) \in K[k]$ and $d, m_0$ be given by (2.3) and (2.4). For any polynomial $x(k) \in K[k]$, let*

$$p(k) = a(k)x(k+1) - b(k-1)x(k).$$

*We have*

$$\deg p(k) \begin{cases} < d+m_0, & \textit{if } (a(k),b(k)) \textit{ is degenerated} \\ & \quad \textit{and } \deg x(k)=m_0, \\ = \deg u(k)+\deg x(k), & \textit{if } x(k) \textit{ is a constant,} \\ = d+\deg x(k), & \textit{otherwise.} \end{cases}$$

**Proof.** If $a(k)=0$, we have $u(k)=-b(k-1)$ and thus

$$\deg p(k)=\deg u(k)+\deg x(k)=d+\deg x(k).$$

Now assume $a(k)\neq 0$. Notice that

$$p(k)=u(k)x(k)+a(k)(x(k+1)-x(k)).$$

If $x(k)$ is a constant, we have $p(k)=u(k)x(k)$ and the assertion holds. Otherwise, we have

$$\deg a(k)(x(k+1)-x(k))=\deg a(k)+\deg x(k)-1.$$

If the leading terms of $u(k)x(k)$ and $a(k)(x(k+1)-x(k))$ do not cancel, the degree of $p(k)$ is $d+\deg x(k)$. Otherwise, we have $\deg u(k)=\deg a(k)-1$ and

$$\operatorname{lc} u(k)+\operatorname{lc} a(k)\cdot \deg x(k)=0,$$

i.e., $\deg x(k)=m_0$. □

It is clear that $S_{a,b}$ is a subspace of $K[k]$, but is not a sub-ring of $K[k]$ in general. Let $[p(k)]=p(k)+S_{a,b}$ denote the coset of a polynomial $p(k)$. We see that the quotient space $K[k]/S_{a,b}$ is finite dimensional.

**Theorem 2.3.** *Let $a(k),b(k)\in K[k]$ and $d,m_0$ be given by (2.3) and (2.4). We have*

$$K[k]/S_{a,b} = \begin{cases} \langle [k^0],[k^1],\ldots,[k^{d-1}],[k^{d+m_0}]\rangle, & \textit{if } (a(k),b(k)) \textit{ is degenerated,} \\ \langle [k^0],[k^1],\ldots,[k^{d}]\rangle, & \textit{if } \deg u(k)<\deg a(k)-1, \\ \langle [k^0],[k^1],\ldots,[k^{d-1}]\rangle, & \textit{otherwise.} \end{cases}$$

**Proof.** If $a(k)=0$, we have

$$S_{a,b}=\{b(k-1)x(k)\colon x(k)\in K[k]\}$$

and $d=\deg b(k)$. Therefore,

$$K[k]/S_{a,b}=\langle [k^0],[k^1],\ldots,[k^{d-1}]\rangle.$$

Now assume $a(k)\neq 0$. For any nonnegative integer $s$, let

$$p_s(k)=a(k)(k+1)^s-b(k-1)k^s.$$

We first consider the case when the pair $(a(k),b(k))$ is not degenerated. By Lemma 2.2, we have

$$\deg p_s(k)=d+s, \quad \forall s\geq 0,$$

except for the case when $\deg u(k)<\deg a(k)-1$ and $s=0$. Suppose that $p(k)$ is a polynomial of degree $m>d$. Then

$$p'(k)=p(k)-\frac{\operatorname{lc} p(k)}{\operatorname{lc} p_{m-d}(k)}p_{m-d}(k) \tag{2.5}$$

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

is a polynomial of degree less than $m$ and $p(k) \in [p'(k)]$. By induction on $m$, we derive that for any polynomial $p(k)$ of degree $> d$, there exists a polynomial $\tilde{p}(k)$ of degree $\leq d$ such that $p(k) \in [\tilde{p}(k)]$. When $\deg u(k) \geq \deg a(k) - 1$, we have $p_0(k) = u(k)$ is of degree $d$ and thus we can further reduce the degree of $\tilde{p}(k)$ by one. Therefore,

$$K[k]/S_{a,b} = \begin{cases} \langle [k^0], [k^1], \ldots, [k^d] \rangle, & \text{if } \deg u(k) < \deg a(k) - 1 \\ \langle [k^0], [k^1], \ldots, [k^{d-1}] \rangle, & \text{otherwise}. \end{cases}.$$

Now we consider the case when $(a(k), b(k))$ is degenerated. By Lemma 2.2,

$$\deg p_s(k) = d + s, \quad \forall s \neq m_0 \quad \text{and} \quad \deg p_{m_0}(k) < d + m_0.$$

The above reduction process (2.5) works well except for the polynomials $p(k)$ of degree $d + m_0$. But in this case,

$$p(k) - \operatorname{lc} p(k) \cdot k^{d+m_0}$$

is a polynomial of degree less than $d + m_0$. Then the reduction process continues until the degree is less than $d$. We thus derive that

$$K[k]/S_{a,b} = \langle [k^0], [k^1], \ldots, [k^{d-1}], [k^{d+m_0}] \rangle,$$

completing the proof. □

**Example 2.1.** Let $n$ be a positive integer and

$$t_k = (-n)_k / k!,$$

where $(\alpha)_k = \alpha(\alpha+1)\cdots(\alpha+k-1)$ is the raising factorial. Then

$$a(k) = k - n, \quad b(k) = k + 1,$$

and

$$S_{a,b} = \{(k-n) \cdot x(k+1) - k \cdot x(k) \colon x(k) \in K[k]\}.$$

We have

$$K[k]/S_{a,b} = \langle [k^n] \rangle$$

is of dimension one.

## 3. The case when $a(k) = -b(k + \alpha)$

In this section, we consider the case when $a(k) = -b(k+\alpha)$ for some $\alpha \in K$ and $b(k)$ has a symmetric property. We will show that in this case, the reduction process maintains the symmetric property. Notice that in this case

$$u(k) = a(k) - b(k-1) = -b(k+\alpha) - b(k-1)$$

has the same degree as $a(k)$, the pair $(a(k), b(k))$ is not degenerated.

We first consider the relation between the symmetric property and the expansion of a polynomial.

**Lemma 3.1.** *Let $p(k) \in K[k]$ and $\beta \in K$. Then the following two statements are equivalent.*

(1) *$p(\beta + k) = p(\beta - k)$ ($p(\beta + k) = -p(\beta - k)$, respectively).*
(2) *$p(k)$ is the linear combination of $(k-\beta)^{2i}$, $i = 0, 1, \ldots$ ($(k-\beta)^{2i+1}$, $i = 0, 1, \ldots$, respectively).*

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

**Proof.** Suppose that

$$p(\beta+k)=\sum_i c_i k^i.$$

Then

$$p(\beta-k)=\sum_i c_i (-k)^i.$$

Therefore,

$$p(\beta+k)=p(\beta-k) \Longleftrightarrow c_{2i+1}=0,\ i=0,1,\ldots.$$

The case of $p(\beta+k)=-p(\beta-k)$ can be proved in a similar way. □

Now we are ready to state the main theorem.

**Theorem 3.2.** *Let $a(k), b(k) \in K[k]$ such that*

$$a(k)=-b(k+\alpha) \quad \textit{and} \quad b(\beta+k)=\pm b(\beta-k),$$

*for some $\alpha, \beta \in K$. Then for any nonnegative integer $m$, we have*

$$[(k+\gamma)^{2m}] \in \left\langle [(k+\gamma)^{2i}] \colon 0 \le 2i < \deg a(k) \right\rangle$$

*and*

$$[(k+\gamma)^{2m+1}] \in \left\langle [(k+\gamma)^{2i+1}] \colon 0 \le 2i+1 < \deg a(k) \right\rangle,$$

*where*

$$\gamma=-\beta+\frac{\alpha-1}{2}. \tag{3.1}$$

**Proof.** We only prove the case of $b(\beta+k)=b(\beta-k)$. The case of $b(\beta+k)=-b(\beta-k)$ can be proved in a similar way. By Lemma 3.1, we may assume that

$$b(k)=b_r(k-\beta)^r+b_{r-2}(k-\beta)^{r-2}+\cdots+b_0,$$

where $r=\deg a(k)=\deg b(k)$ is even and $b_r, b_{r-2}, \ldots, b_0 \in K$ are the coefficients.

Since $(a(k), b(k))$ is not degenerated, taking

$$x(k)=x_s(k)=-\frac{1}{2}\left(k+\gamma-\frac{1}{2}\right)^s, \quad s \in \mathbb{N} \tag{3.2}$$

in Lemma 2.2, we derive that

$$p_s(k)=a(k)x_s(k+1)-b(k-1)x_s(k) \tag{3.3}$$

is a polynomial of degree $s+r$. More explicitly, we have

$$p_s(k)=\frac{1}{2}\left(b(k+\alpha)\left(k+\gamma+\frac{1}{2}\right)^s+b(k-1)\left(k+\gamma-\frac{1}{2}\right)^s\right)$$

is a polynomial with leading term $b_r k^{s+r}$.

Notice that

$$p_s(-\gamma+k)=\frac{1}{2}\left(b(k+\alpha-\gamma)\left(k+\frac{1}{2}\right)^s+b(k-\gamma-1)\left(k-\frac{1}{2}\right)^s\right)$$

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

and

$$p_s(-\gamma-k)=\frac{1}{2}\left(b(-k+\alpha-\gamma)\left(-k+\frac{1}{2}\right)^s+b(-k-\gamma-1)\left(-k-\frac{1}{2}\right)^s\right)$$
$$=\frac{(-1)^s}{2}\left(b(-k+\alpha-\gamma)\left(k-\frac{1}{2}\right)^s+b(-k-\gamma-1)\left(k+\frac{1}{2}\right)^s\right).$$

Since $b(\beta+k)=b(\beta-k)$, i.e., $b(k)=b(2\beta-k)$, we deduce that

$$p_s(-\gamma-k)$$
$$=\frac{(-1)^s}{2}\left(b(2\beta+k-\alpha+\gamma)\left(k-\frac{1}{2}\right)^s+b(2\beta+k+\gamma+1)\left(k+\frac{1}{2}\right)^s\right).$$

By the relation (3.1), we derive that

$$p_s(-\gamma-k)=(-1)^s p_s(-\gamma+k).$$

Suppose that $p(k)$ is a linear combination of the even powers of $(k+\gamma)$ and $\deg p(k)\geq r$. By Lemma 3.1, we have $p(-\gamma-k)=p(-\gamma+k)$ and thus

$$p'(k)=p(k)-\frac{\operatorname{lc}p(k)}{b_r}\cdot p_{\deg p(k)-r}(k)$$

also satisfies $p'(-\gamma-k)=p'(-\gamma+k)$ since $\deg p(k)$ and $r$ are both even. It is clear that $p(k)\in[p'(k)]$ and the degree of $p'(k)$ is less than the degree of $p(k)$. Continuing this reduction process, we finally derive that $p(k)\in[\tilde{p}(k)]$ for some polynomial $\tilde{p}(k)$ with degree $<r$ and satisfying $\tilde{p}(-\gamma-k)=\tilde{p}(-\gamma+k)$. Therefore,

$$[p(k)]\in\langle[(k+\gamma)^{2i}]\colon 0\leq 2i<r\rangle.$$

Suppose that $p(k)$ is a linear combination of the odd powers of $(k+\gamma)$ and $\deg p(k)\geq r$. Then we have $p(-\gamma-k)=-p(-\gamma+k)$ and thus

$$p'(k)=p(k)-\frac{\operatorname{lc}p(k)}{b_r}\cdot p_{\deg p(k)-r}(k)$$

also satisfies $p'(-\gamma-k)=-p'(-\gamma+k)$. Continuing this reduction process, we finally derive that

$$[p(k)]\in\langle[(k+\gamma)^{2i+1}]\colon 0\leq 2i+1<r\rangle.$$

This completes the proof. $\square$

We may further require to express $[(k+\gamma)^m]$ as an integral linear combination of $[(k+\gamma)^i]$, $0\leq i<r$ when $b(k)=(k+1)^r$.

**Theorem 3.3.** *Let*

$$t_k=(-1)^k\left(\frac{(\alpha)_k}{k!}\right)^r,$$

*where $r$ is a positive integer and $\alpha$ is a rational number with denominator $D$. Then for any positive integer $m$, there exist integers $a_0,\ldots,a_{r-1}$ and a polynomial $x(k)\in\mathbb{Z}[k]$ such that*

$$(2Dk+D\alpha)^m t_k=\sum_{i=0}^{r-1}a_i(2Dk+D\alpha)^i t_k+\Delta_k\left(2^{r-1}(Dk)^r x(2Dk)t_k\right).$$

*Moreover, $a_i=0$ if $i\not\equiv m \pmod 2$.*

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

**Proof.** We have

$$\frac{t_{k+1}}{t_k} = \frac{-(k+\alpha)^r}{(k+1)^r}.$$

Let

$$a(k) = -(k+\alpha)^r \quad \text{and} \quad b(k) = (k+1)^r.$$

We see that it is the case of $\beta = -1$ and $\gamma = \alpha/2$ of Theorem 3.2. From (2.1), we derive that

$$\Delta_k(k^r x_s(k) t_k) = p_s(k) t_k, \tag{3.4}$$

where $x_s(k)$ and $p_s(k)$ are given by (3.2) and (3.3) respectively. Multiplying $(2D)^{s+r}$ on both sides, we obtain

$$\Delta_k(2^{r-1}(Dk)^r \tilde{x}_s(2Dk) t_k) = \tilde{p}_s(k') t_k, \tag{3.5}$$

where $k' = 2Dk + D\alpha$,

$$\tilde{x}_s(k) = -(k + D\alpha - D)^s, \tag{3.6}$$

and

$$\tilde{p}_s(k) = \frac{1}{2}\left((k+D\alpha)^r (k+D)^s + (k-D\alpha)^r (k-D)^s\right). \tag{3.7}$$

Notice that $\tilde{x}_s(k), \tilde{p}_s(k) \in \mathbb{Z}[k]$ and $\tilde{p}_s(k)$ is a monic polynomial of degree $s+r$. Moreover, $\tilde{p}_s(k)$ contains only even powers of $k$ or only odd powers of $k$. Using $\tilde{p}_s(k)$ to do the reduction (2.5), we derive that there exist integers $c_m, c_{m-2}, \ldots$ such that

$$p(k) = k^m - c_m \tilde{p}_{m-r}(k) - c_{m-2}\tilde{p}_{m-r-2}(k) - \cdots$$

becomes a polynomial of degree less than $r$. Clearly, $p(k) \in \mathbb{Z}[k]$. Replacing $k$ by $k'$ and multiplying $t_k$, we derive that

$$(k')^m t_k = p(k') t_k + \Delta_k(2^{r-1}(Dk)^r (c_m \tilde{x}_{m-r}(2Dk) + c_{m-2}\tilde{x}_{m-r-2}(2Dk) + \cdots) t_k).$$

Noting that $p(k)$ contains only the monomials of degree $\equiv m \pmod 2$, we complete the proof. □

As an application, we confirm Conjecture 6 of Liu (2019).

**Theorem 3.4.** *Let*

$$S_m = \sum_{k=0}^{\frac{p-1}{2}} (-1)^k (4k+1)^m \left(\frac{(1/2)_k}{(1)_k}\right)^3.$$

*For any positive odd integer m, there exist integers $a_m$ and $c_m$ such that*

$$S_m \equiv a_m \left(p(-1)^{\frac{p-1}{2}} + p^3 E_{p-3}\right) + p^3 c_m \pmod{p^4}$$

*holds for any prime $p \geq 5$.*

**Proof.** Taking $r = 3$ and $\alpha = 1/2$ in Theorem 3.3, there exists an integer $a_m$ and a polynomial $q_m(k) \in \mathbb{Z}[k]$ such that

$$(4k+1)^m t_k - a_m(4k+1)t_k = \Delta_k(32k^3 q_m(4k) t_k),$$

where $t_k = (-1)^k (\frac{1}{2})_k^3/(1)_k^3$. Summing over $k$ from 0 to $\frac{p-1}{2}$, we derive that

$$S_m - a_m S_1 = 32\omega^3 q_m(4\omega)(-1)^{\omega}\left(\frac{(1/2)_\omega}{(1)_\omega}\right)^3,$$

where $\omega = \frac{p+1}{2}$. Noting that

$$\frac{(1/2)_\omega}{(1)_\omega} = p\frac{1}{p+1}\prod_{i=1}^{\frac{p-1}{2}}\frac{2i-1}{2i}$$

and

$$\frac{1}{p+1}\prod_{i=1}^{\frac{p-1}{2}}\frac{2i-1}{2i} = \frac{1}{p+1}\prod_{i=1}^{\frac{p-1}{2}}\frac{p-2i}{2i} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

we have

$$\left(\frac{(1/2)_\omega}{(1)_\omega}\right)^3 \equiv p^3(-1)^{\frac{p-1}{2}} \pmod{p^4}.$$

Hence

$$S_m - a_m S_1 \equiv -32p^3\omega^3 q_m(4\omega) \pmod{p^4}$$

Let $c_m = -4q_m(2)$. We then have

$$S_m \equiv a_m S_1 + p^3 c_m \pmod{p^4}.$$

Sun (2012) proved that for any prime $p \geq 5$,

$$S_1 \equiv (-1)^{\frac{p-1}{2}} p + p^3 E_{p-3} \pmod{p^4}.$$

Therefore,

$$S_m \equiv a_m\left(p(-1)^{\frac{p-1}{2}} + p^3 E_{p-3}\right) + p^3 c_m \pmod{p^4}. \quad \square$$

**Remark 1.** The coefficient $a_m$ and the polynomial $q_m(k)$ can be computed by the extended Zeilberger's algorithm (Chen et al., 2012).

As pointed by one of the referees, Swisher (2015) showed that for any prime $p \geq 5$,

$$\sum_{k=0}^{\frac{bp-1}{a}}(2ak+1)(-1)^k\frac{(1/a)_k^3}{(1)_k^3} \equiv (-1)^{\frac{bp-1}{a}} bp \pmod{p^3},$$

where $a \in \{2, 3, 4\}$ and

$$b = \begin{cases} 1, & p \equiv 1 \pmod{a}, \\ a-1, & p \equiv -1 \pmod{a}. \end{cases}$$

By the same discussion as in the proof of Theorem 3.4, we derive that

**Theorem 3.5.** *Let $a \in \{2, 3, 4\}$. For each odd integer $m$, there exists an integer $a_m$ such that for any prime $p \geq 5$ with $p \equiv \pm 1 \pmod{a}$,*

$$\sum_{k=0}^{\frac{bp-1}{a}}(2ak+1)^m(-1)^k\frac{(1/a)_k^3}{(1)_k^3} \equiv a_m(-1)^{\frac{bp-1}{a}} bp \pmod{p^3},$$

*where*

$$b = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{a}, \\ a-1, & \text{if } p \equiv -1 \pmod{a}. \end{cases}$$

## 4. The case when $a(k) = b(k+\alpha)$

We first give a criterion on the degeneration of $(a(k), b(k))$.

**Lemma 4.1.** *Let $a(k), b(k) \in K[k]$ such that $a(k) = b(k+\alpha)$. Suppose that $-(\alpha+1)\deg a(k) \notin \mathbb{N}$. Then $(a(k), b(k))$ is not degenerated.*

**Proof.** Let $r = \deg a(k) = \deg b(k)$ and

$$u(k) = a(k) - b(k-1) = b(k+\alpha) - b(k-1).$$

It is clear that the coefficient of $k^r$ in $u(k)$ is 0 and the coefficient of $k^{r-1}$ in $u(k)$ is $\mathrm{lc}\, b(k) \cdot (\alpha+1)r$. Since $(\alpha+1)r \neq 0$, we derive that $\deg u(k) = r-1$. Thus,

$$-\mathrm{lc}\, u(k)/\mathrm{lc}\, a(k) = -\mathrm{lc}\, u(k)/\mathrm{lc}\, b(k) = -(\alpha+1)r.$$

Since $-(\alpha+1)r \notin \mathbb{N}$, the pair $(a(k), b(k))$ is not degenerated. $\square$

When $a(k)$ is a shift of $b(k)$, we have a result similar to Theorem 3.2.

**Theorem 4.2.** *Let $a(k), b(k) \in K[k]$ such that*

$$a(k) = b(k+\alpha) \quad \text{and} \quad b(\beta+k) = \pm b(\beta-k),$$

*for some $\alpha, \beta \in K$. Assume further that $-(\alpha+1)\deg a(k) \notin \mathbb{N}$. Then for any nonnegative integer m, we have*

$$[(k+\gamma)^{2m}] \in \left\langle [(k+\gamma)^{2i}]\colon\ 0 \le 2i < \deg a(k) - 1 \right\rangle$$

*and*

$$[(k+\gamma)^{2m+1}] \in \left\langle [(k+\gamma)^{2i+1}]\colon\ 0 \le 2i+1 < \deg a(k) - 1 \right\rangle,$$

*where*

$$\gamma = -\beta + \frac{\alpha-1}{2}.$$

**Proof.** The proof is parallel to the proof of Theorem 3.2. Instead of (3.2), we take

$$x(k) = x_s(k) = \left(k + \gamma - \frac{1}{2}\right)^s$$

in Lemma 2.2. By Lemma 4.1, $(a(k), b(k))$ is not degenerated and

$$\deg(a(k) - b(k-1)) = \deg a(k) - 1.$$

Hence the polynomial

$$p_s(k) = a(k)x_s(k+1) - b(k-1)x_s(k)$$

satisfies

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

$$\deg p_s(k) = s + \deg a(k) - 1.$$

Moreover, we have

$$p_s(-\gamma - k) = \begin{cases} (-1)^{s+1} p_s(-\gamma + k), & \text{if } b(\beta + k) = b(\beta - k), \\ (-1)^s p_s(-\gamma + k), & \text{if } b(\beta + k) = -b(\beta - k), \end{cases}$$

so that the reduction process maintains the symmetric property. Therefore, the reduction process continues until the degree is less than $\deg a(k) - 1$. □

Similar to Theorem 3.3, we have the following result.

**Theorem 4.3.** *Let*

$$t_k = \left( \frac{(\alpha)_k}{k!} \right)^r,$$

*where r is a positive integer and $\alpha$ is a rational number with denominator D. Suppose that $-\alpha r \notin \mathbb{N}$. Then for any positive integer m, there exist integers $a_0, \ldots, a_{r-2}$ and a polynomial $x(k) \in \mathbb{Z}[k]$ such that*

$$(2Dk + D\alpha)^m t_k = \frac{1}{C_m} \sum_{i=0}^{r-2} a_i (2Dk + D\alpha)^i t_k + \frac{1}{C_m} \Delta_k \left( 2^{r-1} (Dk)^r x(2Dk) t_k \right),$$

*where*

$$C_m = \prod_{0 \le 2i \le m-r+1} ((\alpha r + m - r + 1 - 2i) \cdot D).$$

*Moreover, $a_i = 0$ if $i \not\equiv m \pmod 2$.*

**Proof.** The proof is parallel to the proof of Theorem 3.3. Instead of (3.6) and (3.7), we take

$$\tilde{x}_s(k) = (k + D\alpha - D)^s \tag{4.1}$$

and

$$\tilde{p}_s(k) = \frac{1}{2} ((k + D\alpha)^r (k + D)^s - (k - D\alpha)^r (k - D)^s), \tag{4.2}$$

so that (3.5) still holds. It is clear that $\tilde{x}_s(k), \tilde{p}_s(k) \in \mathbb{Z}[k]$. But in this case, $\tilde{p}_s(k)$ is not monic. The leading term of $\tilde{p}_s(k)$ is

$$(\alpha r + s) D \cdot k^{s+r-1}.$$

Now let us consider the reduction process. Let $p(k) \in \mathbb{Z}[k]$ be a polynomial of degree $\ell \ge r - 1$. Assume further that $p(k)$ contains only even powers of $k$ or only odd powers of $k$. Setting

$$\begin{aligned} p'(k) &= \operatorname{lc} \tilde{p}_{\ell-r+1}(k) \cdot p(k) - \operatorname{lc} p(k) \cdot \tilde{p}_{\ell-r+1}(k) \\ &= (\alpha r + \ell - r + 1) D \cdot p(k) - \operatorname{lc} p(k) \cdot \tilde{p}_{\ell-r+1}(k), \end{aligned}$$

we see that $p'(k) \in \mathbb{Z}[k]$ and $\deg p'(k) < \ell$. Since $\tilde{p}_{\ell-r+1}(k)$ contains only even powers of $k$ or only odd powers of $k$, so does $p'(k)$. Therefore, $\deg p'(k) \le \ell - 2$.

Continuing this reduction process until the degree of the resulting polynomial is less than $r - 1$, we finally obtain that there exist integers $c_m, c_{m-2}, \ldots$ such that

$$C_m k^m - c_m \tilde{p}_{m-r+1}(k) - c_{m-2} \tilde{p}_{m-r-1}(k) - \cdots,$$

is a polynomial of degree less than $r-1$ and with integral coefficients, where $C_m$ is the product of the leading coefficients of $\tilde{p}_{m-r+1}(k), \tilde{p}_{m-r-1}(k), \ldots$

$$C_m = \prod_{0 \le 2i \le m-r+1} ((\alpha r + m - r + 1 - 2i)D),$$

as desired. □

For the special case of $t_k = (1/2)_k^4/(1)_k^4$, we may further reduce the factor $C_m$.

**Lemma 4.4.** *Let $m$ be a positive integer and*

$$t_k = \frac{(1/2)_k^4}{(1)_k^4}.$$

- *If $m$ is odd, then there exists an integer $c$ and a polynomial $x(k) \in \mathbb{Z}[k]$ such that*

$$(4k+1)^m t_k = \frac{c}{C'_m}(4k+1)t_k + \frac{1}{C'_m}\Delta_k\left(32k^4 x(4k) t_k\right),$$

  *where $C'_m = (\frac{m-1}{2})!$.*
- *If $m$ is even, then there exist integers $c, c'$ and a polynomial $x(k) \in \mathbb{Z}[k]$ such that*

$$(4k+1)^m t_k = \frac{1}{C'_m}(c + (4k+1)^2 c')t_k + \frac{1}{C'_m}\Delta_k\left(64k^4 x(4k) t_k\right),$$

  *where $C'_m = (m-1)!!$.*

**Proof.** This is the special case of Theorem 4.3 for $\alpha = 1/2$ and $r = 4$. Therefore, $D = 2$ and $\alpha r - r + 1 = -1$.

We need only to show that the coefficients of $\tilde{p}_s(k)$ given by (4.2) are divisible by 2 when $s$ is odd and is divisible by 4 when $s$ is even. Then we may replace $\tilde{x}_s(k)$ given by (4.1) by $\tilde{x}_s(k)/2$ and $\tilde{x}_s(k)/4$, respectively, so that the leading coefficient of $\tilde{p}_s(k)$ is reduced. Correspondingly, the product $C_m$ of the leading coefficients becomes

$$\prod_{0 \le 2i \le m-3} \frac{1}{2} \operatorname{lc} \tilde{p}_{m-3-2i}(k) = \prod_{0 \le 2i \le m-3} (m-1-2i) = (m-1)!!, \quad m \text{ even},$$

and

$$\prod_{0 \le 2i \le m-3} \frac{1}{4} \operatorname{lc} \tilde{p}_{m-3-2i}(k) = \prod_{0 \le 2i \le m-3} \frac{m-1-2i}{2} = \left(\frac{m-1}{2}\right)!, \quad m \text{ odd}.$$

Notice that

$$\tilde{p}_s(k) = \frac{1}{2}((k+1)^4 (k+2)^s - (k-1)^4 (k-2)^s).$$

The coefficient of $k^j$ is

$$\frac{1-(-1)^{s-j}}{2} \sum_{0 \le \ell \le 4,\ 0 \le j-\ell \le s} \binom{4}{\ell}\binom{s}{j-\ell} 2^{s-j+\ell}.$$

If $j - \ell < s$, the corresponding summand is divisible by 2. If $j - \ell = s$ and $\ell$ is even, then $(-1)^{s-j} = 1$ and the coefficient is 0. Otherwise, $\ell = 1$ or $\ell = 3$, and thus $4 \mid \binom{4}{\ell}$. Therefore, the coefficient must be divisible by 2.

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004

Now consider the case of $s$ being even. If $j-\ell < s-1$, the corresponding summand is divisible by 4. Otherwise $j-\ell = s$ or $j-\ell = s-1$. We have seen that if $j-\ell = s$, then the coefficient is divisible by 4. If $j-\ell = s-1$. Then

$$\binom{s}{j-\ell} = s \quad \text{and} \quad 2^{s-j+\ell} = 2.$$

Thus the summand is also divisible by 4. □

**Example 4.1.** Consider the case of $m = 11$. We have

$$(4k+1)^{11} t_k + 10515(4k+1)t_k = \Delta_k(32k^4 p(k) t_k)$$

where

$$p(k) = \frac{1}{5}(4k-1)^8 - \frac{249}{20}(4k-1)^6 + \frac{20207}{60}(4k-1)^4 - \frac{89909}{20}(4k-1)^2 + \frac{524029}{20}.$$

As an application, we obtain the following congruences.

**Theorem 4.5.** *Let m be a positive odd integer and $\mu = (m-1)/2$. Denote*

$$S_m = \sum_{k=0}^{\frac{p-1}{2}} (4k+1)^m \left( \frac{(1/2)_k}{(1)_k} \right)^4 .$$

*Then there exists an integer $a_m$ such that for each prime $p > \mu$,*

$$S_m \equiv \frac{a_m}{\mu!} p \pmod{p^4}.$$

**Proof.** By Lemma 4.4, there exists an integer $a_m$ and a polynomial $q_m(k) \in \mathbb{Z}[k]$ such that

$$(4k+1)^m t_k - \frac{a_m}{\mu!}(4k+1)t_k = \frac{1}{\mu!}\Delta_k \left( 32k^4 q_m(4k) t_k \right),$$

where $t_k = \left( \frac{(1/2)_k}{(1)_k} \right)^4$. Summing over $k$ from 0 to $(p-1)/2$, we obtain

$$S_m - \frac{a_m}{\mu!} S_1 = 32\omega^4 \frac{q_m(4\omega)}{\mu!} \left( \frac{(1/2)_\omega}{(1)_\omega} \right)^4,$$

where $\omega = (p+1)/2$. When $p > \mu$, $1/\mu!$ is a $p$-adic integer and

$$\left( \frac{(1/2)_\omega}{(1)_\omega} \right)^4 \equiv 0 \pmod{p^4}.$$

Therefore,

$$S_m \equiv \frac{a_m}{\mu!} S_1 \pmod{p^4}.$$

It is shown by Long (2011) that

$$S_1 \equiv p \pmod{p^4},$$

completing the proof. □

The integer $a_m$ and the polynomial $q_m(k)$ can be computed by the extended Zeilberger's algorithm. By checking the initial values, we propose the following conjecture.

**Conjecture 4.6.** *For any positive odd integer m, the coefficient $a_m/(\frac{m-1}{2})!$ is an integer.*

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgement

The work was supported by the National Natural Science Foundation of China (grants 11471244, 11771330 and 11701420). We thank the referees for their valuable comments and suggestions.

## References

Abramov, S.A., 1975. The rational component of the solution of a first-order linear recurrence relation with rational right-hand side. Comput. Math. Math. Phys. 15, 1035–1039.
Abramov, S.A., 1995. Indefinite sums of rational functions. In: Proc. ISSAC'95. ACM Press, New York, pp. 303–308.
Abramov, S.A., Petkovšek, M., 2001. Minimal decomposition of indefinite hypergeometric sums. In: Proc. ISSAC'2001. ACM Press, New York, pp. 7–14.
Abramov, S.A., Petkovšek, M., 2002. Rational normal forms and minimal decompositions of hypergeometric terms. J. Symb. Comput. 33, 521–543.
Ahlgren, S., Ono, K., 2000. A Gaussian hypergeometric series evaluation and Apéry number congruences. J. Reine Angew. Math. 518, 187–212.
Chen, S., Huang, H., Kauers, M., Li, Z., 2015. A modified Abramov-Petkovšek reduction and creative telescoping for hypergeometric terms. In: Proc. ISSAC'2015. ACM Press, New York.
Chen, W.Y.C., Hou, Q.-H., Mu, Y.-P., 2012. The extended Zeilberger algorithm with parameters. J. Symb. Comput. 47 (6), 643–654.
Guo, V.J.W., 2017. Some generalizations of a supercongruence of van Hamme. Integral Transforms Spec. Funct. 28 (12), 888–899.
Guo, V.J.W., 2019. Common $q$-analogues of some different supercongruences. Results Math. 74 (4), 131.
Jana, A., Kalita, G., 2019. Supercongruences for sums involving rising factorial $(\frac{1}{\ell})_k^3$. Integral Transforms Spec. Funct. 30 (9), 683–692.
Liu, J.-C., 2019. Semi-automated proof of supercongruences on partial sum of hypergeometric series. J. Symb. Comput. 93, 221–229.
Long, L., 2011. Hypergeometric evaluation identities and supercongruences. Pac. J. Math. 249, 405–418.
Mortenson, E., 2008. A $p$-adic supercongruence conjecture of van Hamme. Proc. Am. Math. Soc. 136, 4321–4328.
Osburn, R., Schneider, C., 2009. Gaussian hypergeometric series and supercongruences. Math. Comput. 78 (265), 275–292.
Osburn, R., Sahu, B., Straub, A., 2016. Supercongruences for sporadic sequences. Proc. Edinb. Math. Soc. 59 (2), 503–518.
Pirastu, R., Strehl, V., 1995. Rational summation and Gosper-Petkovšek representation. J. Symb. Comput. 20, 617–635.
Sun, Z.-W., 2012. A refinement of a congruence result by van Hamme and Mortenson. Ill. J. Math. 56, 967–979.
Sun, Z.-W., 2013. Supercongruences involving products of two binomial coefficients. Finite Fields Appl. 22, 24–44.
Sun, Z.-W., 2014. On sums related to central binomial and trinomial coefficients. In: Nathanson, M.B. (Ed.), Combinatorial and Additive Number Theory: CANT 2011 and 2012. In: Springer Proc. Math. & Stat., vol. 101. Springer, New York, pp. 257–312.
Swisher, H., 2015. On the supercongruence conjectures of van Hamme. Res. Math. Sci. 2 (1), 18.
van Hamme, L., 1997. Some conjectures concerning partial sums of generalized hypergeometric series. In: $p$-Adic Functional Analysis. Nijmegen, 1996. In: Lecture Notes in Pure and Appl. Math., vol. 192. Dekker, pp. 223–236.
Wang, S.-D., 2018. Some supercongruences involving $\binom{2k}{k}^4$. J. Differ. Equ. Appl. 24 (9), 1375–1383.
Zudilin, W., 2009. Ramanujan-type supercongruences. J. Number Theory 129, 1848–1857.

Please cite this article in press as: Hou, Q.-H., et al. Polynomial reduction and supercongruences. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.11.004