SIMPLER MALTSEV CONDITIONS FOR (WEAK) DIFFERENCE TERMS IN LOCALLY FINITE VARIETIES

KEITH KEARNES, ÁGNES SZENDREI, AND ROSS WILLARD

Abstract. This paper is motivated by a practical question: given a finite algebra $\mathbf{A}$ in a finite language, how can we best program a computer to decide whether the variety generated by $\mathbf{A}$ has a difference term, and how hard is it to find the difference term? To help address this question we produce a simple Maltsev condition which characterizes difference terms in the class of locally finite varieties. We do the same for weak difference terms.

Let $\mathcal{V}$ be a variety. A 3-ary term $p(x, y, z)$ is said to be a *weak difference term* for $\mathcal{V}$ if it is idempotent and satisfies the Maltsev identities $p(x, x, y) \approx y \approx p(y, x, x)$ whenever p is restricted to a block of an abelian congruence of a member of $\mathcal{V}$. A weak difference term which moreover satisfies $\mathcal{V} \models p(x, x, y) \approx y$ is called a *difference term* for $\mathcal{V}$.

Difference terms and weak difference terms are ubiquitous. Every congruence modular variety [1] or congruence meet-semidistributive variety (trivially) has a difference term. A locally finite variety omits type 1 in the sense of tame congruence theory if and only if it has a weak difference term [2, Theorem 9.6]. Difference terms and weak difference terms can be characterized, in principle, by Maltsev conditions involving additional 3-ary terms ([5, Theorem 8.8], [6, Theorem 1.2(2)]) which in turn imply reasonably simple syntactic characterizations [6, Theorem 1.2(3)], [8, Theorem 2.1(4)], similar in form to the third author's syntactic characterization of congruence meet-semidistributive varieties [7, Theorem 2.1].

These characterizing Maltsev conditions have never been explicitly worked out; however, it was shown in [5, Theorem 5.5] that if a locally finite variety has a weak difference term, then it has one which is witnessed by a Maltsev condition that is significantly simpler than the characterizing condition. A similar improvement for difference terms in locally finite varieties was announced without proof in [6]. In this paper we further improve these results to the point where the witnessing Maltsev conditions can be easily described. We also give a family of examples to show that

---

Date: `locfin-diffterm_final.tex`, revised September 6, 2016.

This material is based upon work supported by the National Science Foundation grant no. DMS 1500254 and the Hungarian National Foundation for Scientific Research (OTKA) grant no. K104251 and K115518. The third author acknowledges the support of the Natural Sciences and Engineering Research Council of Canada.

there is no uniform derivation of a weak difference term from a Siggers-like operation, even in locally finite varieties.

1. Simple Maltsev conditions

Following [5, Def. 5.2], given congruences α, β, γ of an algebra, define $\tau(\alpha, \beta, \gamma)$ to be the transitive closure of $\beta \cup (\alpha \cap (\gamma \circ (\alpha \cap \beta) \circ \gamma))$. Our first result slightly improves [5, Theorem 5.5], and improves [8, Theorem 2.1] in the case of locally finite varieties.

Theorem 1. *Let $\mathcal{V}$ be a variety for which $\mathbf{F}_{\mathcal{V}}(2)$ is finite. The following are equivalent:*

(1) *$\mathcal{V}$ has a weak difference term.*
(2) *For all $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$,*

$$\alpha \cap (\beta \circ \gamma) \subseteq \tau^* \circ \tau$$

where $\tau = \tau(\alpha, \beta, \gamma)$ and $\tau^* = \tau(\alpha, \gamma, \beta)$.
(3) *For some $n \geq 1$ there exist idempotent terms $f_i(x, y, z), g_i(x, y, z)$, $1 \leq i \leq 4n$, and $p(x, y, z)$ such that the following are identities of $\mathcal{V}$:*

$$\begin{aligned}
f_i(x,y,x) &\approx g_i(x,y,x) \quad \textit{for all } i \\
x &\approx f_1(x,y,y) \\
g_i(x,y,y) &\approx f_{i+1}(x,y,y) \quad \textit{for } 1 \leq i < n \\
f_i(x,x,y) &\approx f_{2n+i}(x,x,y) \quad \textit{for } 1 \leq i \leq n \\
g_i(x,x,y) &\approx g_{2n+i}(x,x,y) \quad \textit{for } 1 \leq i \leq n \\
f_{2n+i}(x,y,y) &\approx g_{2n+i}(x,y,y) \quad \textit{for } 1 \leq i \leq n \\
g_n(x,y,y) &\approx p(x,y,y) \\
p(x,x,y) &\approx f_{n+1}(x,x,y) \\
g_{n+i}(x,x,y) &\approx f_{n+i+1}(x,x,y) \quad \textit{for } 1 \leq i < n \\
f_{n+i}(x,y,y) &\approx f_{3n+i}(x,y,y) \quad \textit{for } 1 \leq i \leq n \\
g_{n+i}(x,y,y) &\approx g_{3n+i}(x,y,y) \quad \textit{for } 1 \leq i \leq n \\
f_{3n+i}(x,x,y) &\approx g_{3n+i}(x,x,y) \quad \textit{for } 1 \leq i \leq n \\
g_{2n}(x,x,y) &\approx y
\end{aligned}$$

Moreover, if f_i, g_i, p are terms satisfying the identities in (3)*, then p is a weak difference term for $\mathcal{V}$ and the pairs $\{(f_i, g_i), (f_i^{\mathrm{rev}}, g_i^{\mathrm{rev}}) : 1 \leq i \leq 4n\}$ witness* [8, Theorem 2.1(4)] *for p, where $h^{\mathrm{rev}}(x, y, z) := h(z, y, x)$.*

Remark 2. We do not claim that (and do not know whether) every weak difference term p for $\mathcal{V}$ is accompanied by terms f_i, g_i satisfying (with p) the identities in Theorem 1(3). In particular, we do not know if a locally finite variety which omits

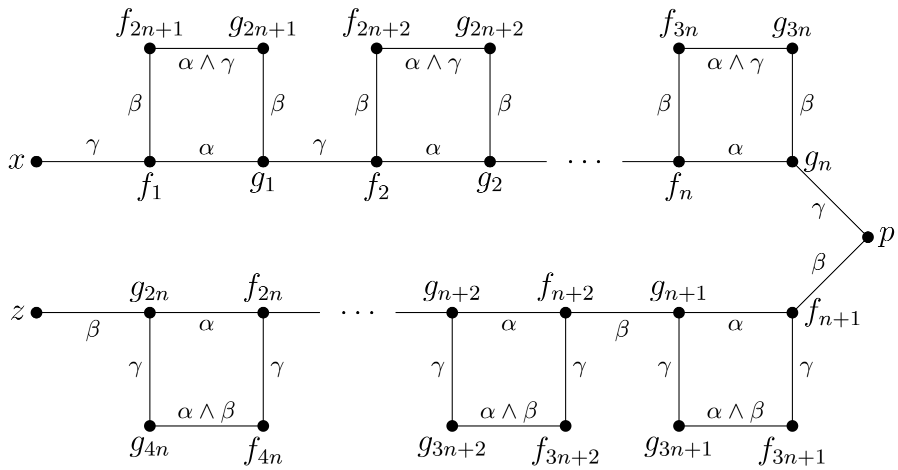

FIGURE 1

type 1 has a weak difference term simultaneously satisfying (3) and which is Maltsev on every block of a locally solvable congruence in $\mathcal{V}$ (cf. [2, Theorem 9.6]).

Proof. Given congruences α, β, γ of an algebra, define $\beta_2 = \beta \vee (\alpha \wedge (\gamma \vee (\alpha \wedge \beta)))$ and $\gamma_2 = \gamma \vee (\alpha \wedge (\beta \vee (\alpha \wedge \gamma)))$. Clearly $\tau(\alpha, \beta, \gamma) \leq \beta_2$ and $\tau(\alpha, \gamma, \beta) \leq \gamma_2$. Hence (2) $\Rightarrow$ (1) is an immediate consequence of [5, Theorem 5.5(2 $\Rightarrow$ 1)]. In fact, the proof of [5, Theorem 5.5(1 $\Rightarrow$ 2)] with minor adjustments also proves (1) $\Rightarrow$ (2). The equivalence of (2) with (3) is valid for arbitrary varieties and is shown in the usual way, by specializing (2) to $\mathbf{A} = \mathbf{F}_{\mathcal{V}}(x, y, z)$, $\alpha = \mathrm{Cg}^{\mathbf{A}}(x, z)$, $\beta = \mathrm{Cg}^{\mathbf{A}}(x, y)$, and $\gamma = \mathrm{Cg}^{\mathbf{A}}(y, z)$. (See Figure 1.)

Finally, if f_i, g_i, p are terms satisfying the identities in (3), then for any $\mathbf{A} \in \mathcal{V}$ and $a, b \in A$, if $f_i(a, a, b) = g_i(a, a, b) \leftrightarrow f_i(a, b, b) = g_i(a, b, b)$ for all $1 \leq i \leq 4n$, then from the identities in (3) we can easily deduce $a = p(a, b, b)$ and $p(a, a, b) = b$. Symmetrically, if $f_i^{\mathrm{rev}}(a, a, b) = g_i^{\mathrm{rev}}(a, a, b) \leftrightarrow f_i^{\mathrm{rev}}(a, b, b) = g_i^{\mathrm{rev}}(a, b, b)$ for all $1 \leq i \leq 4n$, then $b = p(b, a, a)$ and $p(b, b, a) = a$. This establishes that the pairs $\{(f_i, g_i), (f_i^{\mathrm{rev}}, g_i^{\mathrm{rev}}))\ :\ 1 \leq i \leq 4n\}$ witness [8, Theorem 2.1(4)]. By adapting the proof of [6, Theorem 1.2(3 $\Rightarrow$ 1)], one can deduce that p is a weak difference term. $\square$

The next theorem is shown by combining results of the first two authors [3, 5]. It slightly improves an observation made in passing at the end of Section 1 in [6].

Theorem 3. *Let $\mathcal{V}$ be a variety for which $\mathbf{F}_{\mathcal{V}}(2)$ is finite. The following are equivalent:*

(1) *$\mathcal{V}$ has a difference term.*
(2) *For all $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$,*

$$\alpha \cap (\beta \circ \gamma) \subseteq (\alpha \cap \tau) \circ \gamma \circ \beta$$

where $\tau = \tau(\alpha, \beta, \gamma)$.

(3) *For some* $n \geq 1$ *there exist idempotent terms* $f_i(x, y, z), g_i(x, y, z)$, $0 \leq i \leq 2n$, *and* $p(x, y, z)$ *such that the following are identities of* $\mathcal{V}$*:*

$$\begin{aligned}
f_0(x,y,z) &\approx x \\
f_0(x,x,y) &\approx f_1(x,x,y) \quad \text{and} \quad g_0(x,x,y) \approx g_n(x,x,y) \\
f_i(x,y,x) &\approx g_i(x,y,x) \quad \text{for all } i \leq 2n \\
g_i(x,x,y) &\approx f_{i+1}(x,x,y) \quad \text{for } 1 \leq i < n \\
f_{n+i}(x,x,y) &\approx g_{n+i}(x,x,y) \quad \text{for } 1 \leq i \leq n \\
f_i(x,y,y) &\approx f_{n+i}(x,y,y) \quad \text{for } 1 \leq i \leq n \\
g_i(x,y,y) &\approx g_{n+i}(x,y,y) \quad \text{for } 1 \leq i \leq n \\
g_0(x,y,y) &\approx p(x,y,y) \quad \text{and} \quad p(x,x,y) \approx y.
\end{aligned}$$

Moreover, if f_i, g_i, p *are terms satisfying the identities in* (3)*, then* p *is a difference term for* $\mathcal{V}$ *and the pairs* (f_i, g_i) *witness* [6, Theorem 1.2(3)] *for* p.

Remark 4. We do not claim that (and do not know whether) every difference term p for $\mathcal{V}$ is accompanied by terms f_i, g_i satisfying (with p) the identities in Theorem 3(3).

Proof. (2) $\Leftrightarrow$ (3) is established in the standard way (see Figure 2), and (2) $\Rightarrow$ (1) follows from [6, Theorem 1.2 (2) $\Rightarrow$ (1)] because $\tau \leq \beta_2 := \beta \vee (\alpha \wedge (\gamma \vee (\alpha \wedge \beta)))$.

To prove (1) $\Rightarrow$ (3), we can replace $\mathcal{V}$ by the subvariety of $\mathcal{V}$ generated by $\mathbf{F}_{\mathcal{V}}(2)$, since the identities in (3) are two-variable identities. Thus we can assume that $\mathcal{V}$ is locally finite. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and as usual let $\alpha = \mathrm{Cg}^{\mathbf{F}}(x, z)$, $\beta = \mathrm{Cg}^{\mathbf{F}}(x, y)$ and $\gamma = \mathrm{Cg}^{\mathbf{F}}(y, z)$. Also let $\tau = \tau(\alpha, \beta, \gamma)$. By finiteness of $\mathbf{F}$ and [5, Lemma 5.3], $\alpha - \tau$ contains no 2-snags, so α is solvable over $\alpha \wedge \tau$ by [2, Theorem 7.2]. Hence there exists $m \geq 0$ such that so that $[\alpha]^m \leq \tau$.

By [3, Lemma 2.7], there exists a term $p(x, y, z)$ such that $\mathcal{V} \models p(x, x, y) \approx y$ and $(x, p^{\mathbf{F}}(x, z, z)) \in [\alpha]^m$. Hence $(x, p^{\mathbf{F}}(x, z, z)) \in \alpha \cap \tau$, so $(x, z) \in (\alpha \cap \tau) \circ \gamma \circ \beta$ witnessed by $p^{\mathbf{F}}(x, z, z)$ and $p^{\mathbf{F}}(x, y, z)$. The identities then follow in the standard way, and the "Moreover" claim follows from arguments in [6, Theorem 1.2]. $\square$

The theorems above hold in particular for varieties where $\mathbf{F}_{\mathcal{V}}(3)$ is finite. For a variety $\mathcal{V}$ of this form, it follows from [4, Theorem 2.2] that $\mathcal{V}$ has a weak difference term if and only if it has a 4-ary "Siggers-like" term t, which is a term such that

$$\mathcal{V} \models t(x, x, x, x) \approx x \quad \text{and} \quad \mathcal{V} \models t(x, y, z, y) \approx t(y, z, x, x).$$

This condition from [4] involves a single 4-ary term and two identities, while our current Theorem 1, which characterizes the same class of varieties, involves an unbounded number of terms and identities. One might wonder whether there is a direct way to construct the terms of Theorem 1, or even just the weak difference term of

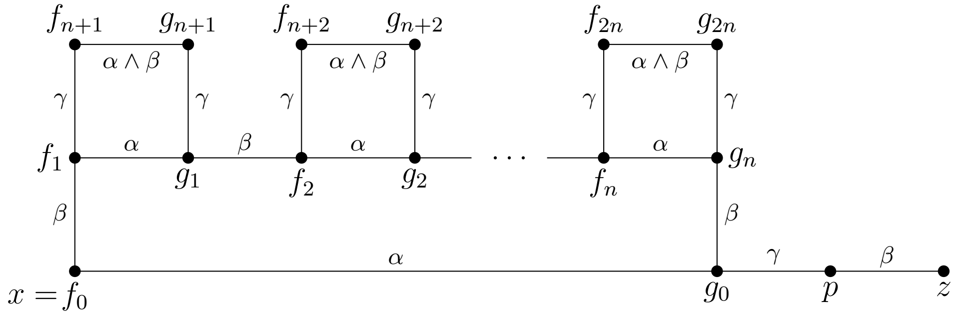

FIGURE 2

that theorem, from a Siggers-like term. We explain now why there no is uniform procedure to do this.

The argument we sketch shows that, given any positive integer k, there is a locally finite variety with a 4-ary Siggers-like term t such that no weak difference term of the variety that is constructible from t has a term tree of depth $\leq k$. For this argument we assume that t is a fundamental operation of the variety, and use the fact that any term constructible from an idempotent fundamental operation t with a term tree of depth $\leq k$ may be obtained from the k-fold "$*$-product" $t * \cdots * t$ by identification of variables. Here the $*$-product of an m-ary operation f and an n-ary operation g is defined to be the operation

$$f(g(x_{11}, x_{12}, \ldots, x_{1n}), \ldots, g(x_{m1}, x_{m2}, \ldots, x_{mn})),$$

which is created by applying g to each of the rows of an $m \times n$ matrix of distinct variables and then applying f to the resulting values.

So fix $k \geq 1$ and let p be a prime of the form $2^{k+1} \cdot d - 1$ with $d \geq 1$. Such a prime exists for any k and d by Dirichlet's Theorem on primes in arithmetic progression. Now define a 4-ary Siggers-like term on $\mathbb{Z}_p$ by

$$t(w, x, y, z) = 2^k d \cdot (w + z) = \frac{p+1}{2}(w + z) \equiv \frac{w + z}{2} \pmod{p}.$$

On $\mathbb{Z}_p$, the operation t agrees with a group term operation that has two equal nonzero coefficients which sum to 1 modulo p, namely coefficients $2^k d$. It follows that on $\mathbb{Z}_p$ the k-fold $*$-product of copies of t has 2^k equal nonzero coefficients which sum to 1 modulo p; these coefficients are equal to $2d$, which is strictly greater than 1. By renaming variables we may write this operation as $2d \sum_{i=1}^{2^k} x_i$. Our goal is to show that it is not possible to obtain a weak difference term from this operation by identification of variables.

The operation $2d \sum_{i=1}^{2^k} x_i$ belongs to the clone of the abelian group $\mathbb{Z}_p$, and this clone contains a unique weak difference operation, namely the Maltsev term $x - y + z$.

If this weak difference operation can be obtained by setting variables in $2d\sum_{i=1}^{2^k} x_i$ to the values x, y and z, then it must be possible to partition the variables into 3 groups so that the sum of the coefficients in the three groups are the coefficients $+1, -1, +1$ of the operation $x - y + z$. That is, it must be possible to partition the 2^k nonzero coefficients into groups of size u, v, w, each a positive number, so that $u + v + w = 2^k$ and the sums over the classes are $+1, -1, +1 \pmod p$ respectively. These sums are $2du, 2dv$ and $2dw$ respectively. Since $2du \geq 2d > 1$ and $2du \equiv +1 \pmod p$ we must have $2du \geq p + 1 = 2^{k+1}d$ in $\mathbb{Z}$, or $u \geq 2^k$. Similarly $v \geq 2^k - 1$ and $w \geq 2^k$. This contradicts the fact that $u + v + w = 2^k$. This proves that $x - y + z$ cannot be obtained by identifying variables in a k-fold $*$-product of copies of t.

References

[1] Christian Herrmann, Affine algebras in congruence modular varieties, *Acta Sci. Math. (Szeged)* **41** (1979), 119–125.

[2] David Hobby and Ralph McKenzie, *The Structure of Finite Algebras*. Contemp. Math. **76**, Amer. Math. Soc., 1988.

[3] Keith A. Kearnes, Varieties with a difference term, *J. Algebra* **177** (1995), 926–960.

[4] Keith Kearnes, Petar Marković, and Ralph McKenzie, Optimal strong Mal'cev conditions for omitting type 1 in locally finite varieties, *Algebra Universalis* **72** (2014), 91–100.

[5] Keith A. Kearnes and Ágnes Szendrei, The relationship between two commutators, *Internat. J. Algebra Comput.* **8** (1998), 492–531.

[6] Keith Kearnes, Ágnes Szendrei, and Ross Willard, A finite basis theorem for difference-term varieties with a finite residual bound, *Trans. Amer. Math. Soc.* **368** (2016), 2115–2143.

[7] Ross Willard, A finite basis theorem for residually finite, congruence meet-semidistributive varieties, *J. Symbolic Logic* **65** (2000), 187–200.

[8] Alexander Wires, A quasi-Mal'cev condition with unexpected application, *Algebra Universalis* **73** (2015), 335–346.