Powers and alternative laws

Nicholas Ormes, Petr Vojtěchovský

Abstract. A groupoid is alternative if it satisfies the alternative laws $x(xy) = (xx)y$ and $x(yy) = (xy)y$. These laws induce four partial maps on $\mathbb{N}^+ \times \mathbb{N}^+$

$$(r,\, s) \mapsto (2r,\, s-r), \quad (r-s,\, 2s), \quad (r/2,\, s+r/2), \quad (r+s/2,\, s/2),$$

that taken together form a dynamical system. We describe the orbits of this dynamical system, which allows us to show that nth powers in a free alternative groupoid on one generator are well-defined if and only if $n \leq 5$. We then discuss some number theoretical properties of the orbits, and the existence of alternative loops without two-sided inverses.

Keywords: alternative laws, alternative groupoid, powers, dynamical system, alternative loop, two-sided inverse

Classification: Primary 20N02; Secondary 20N05, 37E99

1. Alternative laws and the induced dynamical systems

Let G be a free groupoid with one generator x. The elements of G are (correctly parenthesized) words built from the single letter x. The *length* $|w|$ of a word w is the number of letters in w.

For a positive integer n we denote by x^n any of the words of length n in G. Note that there are precisely c_n such words, where c_n is the nth *Catalan number* defined by the recursive relation $c_0 = 1$, $c_1 = 1$, $c_{n+1} = c_1c_n + c_2c_{n-1} + \cdots + c_{n-1}c_2 + c_nc_1$, cf. [7].

A groupoid is said to be *left alternative* if it satisfies the left alternative law $x(xy) = (xx)y$. Dually, it is *right alternative* if it satisfies the right alternative law $x(yy) = (xy)y$. A groupoid that is both left alternative and right alternative is called *alternative*. (When dealing with algebras, the *flexible law* $x(yx) = (xy)x$ is counted among alternative laws, and hence alternative algebras by definition satisfy the flexible law in addition to the left and right alternative laws. Our terminology is common for nonassociative structures with one binary operation.)

Both authors supported by the 2004 PROF Grant of the University of Denver.

Let A be the free alternative groupoid with generator x. Then A consists of equivalence classes of G, where two elements of G are equivalent if and only if they can be obtained from each other by finitely many applications of the alternative laws. For instance, the equivalence class of $(xx)(xx)$ consists of all possible powers x^4, as is immediately seen from $x((xx)x) = x(x(xx)) = (xx)(xx) = ((xx)x)x = (x(xx))x$ and from the fact that $c_4 = 5$. Thus the words of the form x^4 form an equivalence class in A, i.e., x^4 is *well-defined*.

The goal of this paper is to determine for which $n > 0$ the power x^n is well-defined in A, and to investigate related questions. In Sections 5 and 6 we turn our attention to alternative loops without two-sided inverses. The following concept proves useful in all of these tasks:

Consider a word $w = uv$ in G such that $|u| = r > 0$, $|v| = s > 0$. Assume that w is transformed into $w' = u'v'$ by a single application of an alternative law. Then $(|u'|, |v'|)$ is either (r, s) (when the law is applied inside u or v), or $(2r, s-r)$ (when $w = u(ut)$), or $(r-s, 2s)$ (when $w = (tv)v$), or $(r/2, s+r/2)$ (when $w = (tt)v$), or $(r+s/2, s/2)$ (when $w = u(tt)$). This suggests the introduction of these partial maps on $\mathbb{N}^+ \times \mathbb{N}^+$:

$$\alpha(r,s) = (2r, s-r), \qquad \beta(r,s) = (r-s, 2s),$$
$$\gamma(r,s) = (r/2, s+r/2), \qquad \delta(r,s) = (r+s/2, s/2).$$

Note that α is defined if and only if $s > r$, β is defined if and only if $r > s$, γ is defined if and only if r is even, and δ is defined if and only if s is even. Also note that α is the inverse of γ, and β is the inverse of δ (in the sense that $\alpha\circ\gamma$, $\gamma\circ\alpha$, $\beta\circ\delta$, $\delta\circ\beta$ are identity maps on their respective domains).

It is not a novel idea to think of partial maps on integers as a dynamical system — the most notorious example being the dynamical system on $\mathbb{N}^+$ associated with the $3n+1$ problem [8]. In that case there are two maps

$$\mu(r) = \frac{r}{2},$$
$$\nu(r) = \frac{3r+1}{2},$$

μ is defined for even r, ν for odd r, and the (open) problem is whether 1 can be found in the orbit of every r.

Just as in the $3n+1$ problem, we are interested in the orbits of the dynamical system. We define the *orbit* of $(r,s) \in \mathbb{N}^+ \times \mathbb{N}^+$ as the set

$$O(r,s) = \{\varphi_k\varphi_{k-1}\cdots\varphi_1(r,s);\ k \geq 0,\ \varphi_i \in \{\alpha,\ \beta,\ \gamma,\ \delta\}\}.$$

Note that although the dynamical system is defined on $\mathbb{N}^+ \times \mathbb{N}^+$, it is really a union of one-dimensional dynamical systems, since $a + b = r + s$ for every $(a,b) \in O(r,s)$.

The orbits do not capture the equivalence classes of G, of course, but they provide some information about them. In particular, if $u_1v_1 = u_2v_2$ in A, then $(|u_1|, |v_1|) \in O(|u_2|, |v_2|)$.

More information about A can be recovered by considering higher dimensional dynamical systems. For an integer $m > 1$, let T denote all binary trees with m leaves. Let $t \in T$ be one of the trees and $w = u_1 \cdots u_m$ a word bracketed according to t, with $|u_i| = r_i$. Then the alternative laws apply to w and produce words bracketed according to some $t' \in T$ with subwords of some lengths $r'_1, \dots, r'_m$. The *orbit* of $(r_1, \dots, r_m) \in (\mathbb{N}^+)^m$ then consists of all m-tuples $(r'_1, \dots, r'_m)$ obtained as above from all trees $t \in T$ and all words w bracketed according to t with subwords of lengths $r_1, \dots, r_m$.

In full generality, the structures that describe the action of identities on terms are known as geometry monoids, with which one can associate so-called syntactical monoids. See [2], [3], [4].

When $m = 2$, we do not have to worry about all possible bracketings, since the two top factors are uniquely specified in a given word of G. Since we will need the dynamical systems of dimension $m > 2$ only on one occasion (Lemma 3.6), we do not discuss them here any further.

2. Orbits

We are now going to describe the general shape of any orbit $O(r, s)$. The key observation is the following:

When $r < s$ then α applies to (r, s) and

$$\alpha(r, s) = (2r, s - r) = (2r \mod (r + s),\ 2s \mod (r + s)).$$

When $r > s$ then β applies to (r, s) and

$$\beta(r, s) = (r - s, 2s) = (2r \mod (r + s),\ 2s \mod (r + s)).$$

Hence the two partial maps α, β can be replaced by a single partial map ω on $\mathbb{N}^+ \times \mathbb{N}^+$ given by

$$\omega(r, s) = (2r \mod (r + s),\ 2s \mod (r + s)),$$

defined if and only if $r \neq s$. Moreover, since α is the inverse of γ, and β is the inverse of δ, ω is the left inverse of both γ and δ. (This peculiarity arises because γ, δ are not defined everywhere.)

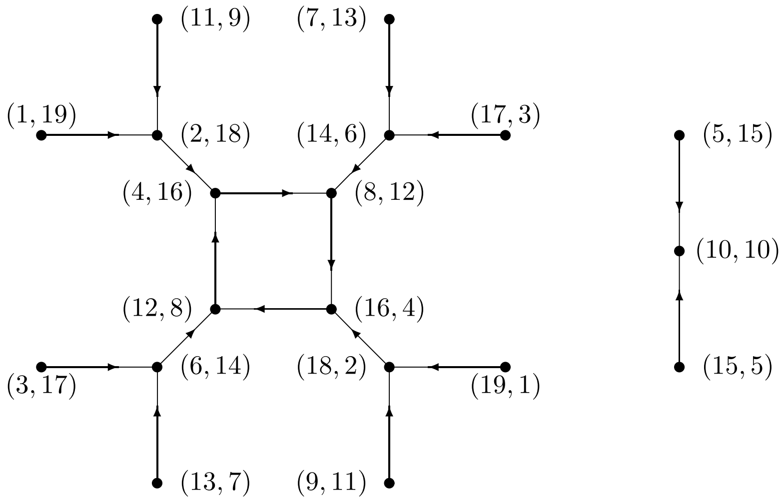

Figure 1. Orbits for $n = r + s = 20$.

Figure 1 shows all (two) orbits $O(r,s)$ with $r + s = 20$. The arrows in the figure stand for a single application of ω. All features of orbits that we are going to discuss are already displayed in the figure.

Lemma 2.1. *Let $a, b, r, s > 0$. Then $(a, b) \in O(r, s)$ if and only if there are $m, n \in \mathbb{N}$ such that $\omega^m(a, b) = \omega^n(r, s)$.*

Proof: Every map φ_i in the definition of $O(r, s)$ is either ω, or a right inverse of ω. On any path from (r, s) to (a, b) in the orbit, a right inverse of ω cannot be followed by ω, of course. Hence there is at most one point along the path where ω is followed by a right inverse of ω. □

Let O be an orbit and $g > 0$ an integer. We say that a point $v = (r, s) \in O$ *has depth* g (or *is at depth* g) if $\gcd(r, s) = g$. We also denote the depth of v by $\gcd(v)$, and define $\gcd(V) = \max_{v\in V} \gcd(v)$ for any subset V of O. In particular, $\gcd(O)$ is the *depth* of O. The subset of O consisting of all $v \in O$ of maximum depth will be called the *bottom* of O, and denoted by $B = B(O)$.

Lemma 2.2. *Let $r, s > 0$, $r \neq s$, $r+s = n = 2^a b$, b odd. Let $g = \gcd(r, s) = 2^c d$, d odd, and $(r', s') = \omega(r, s)$. Then $g' = \gcd(r', s') \in \{g, 2g\}$, and $g' = g$ if and only if $a = c$.*

Proof: Without loss of generality, let $r' = 2r$, $s' = s - r$ (i.e., $\omega = \alpha$). Since g is a common divisor of r, s, it is also a common divisor of r', s', and thus $g|g'$. It then follows that $g' \in \{g, 2g\}$, because $\gcd(r, s) = \gcd(r, s')$ and $r' = 2r$.

When $a = c$ then $g' \neq 2g$ (equivalently, $g' = g$) because g' is a divisor of $n = r' + s'$ but $2g$ is not. When $a > c$ then $g' = 2g$ because both $r' = 2r$ and $s' = n - r'$ are divisible by $2g$. □

Hence the depth increases by the factor of 2 with every application of ω until the bottom is reached.

Corollary 2.3. *Let $r, s > 0$, $(a, b) \in O(r, s)$. Then $\gcd(a, b)/\gcd(r, s) = 2^m$ for some $m \in \mathbb{Z}$.*

Lemma 2.4. *Let $r, s > 0$, $r + s = n$, and $g = \gcd(r, s)$. Then exactly one of the following is true:*

(i) *g is odd, n is even, and (r, s) has no ω-preimages,*
(ii) *both g, n are odd, (r, s) has one ω-preimage (r', s'), and $\gcd(r', s') = g$,*
(iii) *g is even and (r, s) has two ω-preimages (r', s'), (r'', s'').*

Furthermore, if (iii) *holds and $g' = \gcd(r', s') = \gcd(r'', s'')$ then $g = 2g'$.*

Proof: First note that the case g even, n odd cannot occur.

An ω-preimage of (r, s) has two possible forms: $\gamma(r, s) = (r/2, s + r/2) = (r/2, (s + n)/2)$, or $\delta(r, s) = (r + s/2, s/2) = ((r + n)/2, s/2)$.

When g is odd and n is even then both r and s are odd, so neither $r/2$ nor $s/2$ are integers, and (r, s) has no ω-preimages.

When g and n are both odd then one of r, s is even and the other is odd. Without loss of generality assume that r is even and s is odd. Then $r' = r/2$, $s' = (s+n)/2$ are integers, and (r', s') is the unique ω-preimage of (r, s). Moreover, $g = \gcd(r, s) = \gcd(r, s + n) = \gcd(r/2, (s + n)/2)$ since g is odd.

Assume that g is even. Then n, r, s are all even. Hence $(r', s') = (r/2, (s + n)/2)$, $(r'', s'') = ((r + n)/2, s/2)$ are ω-preimages of (r, s).

Assume further that $g' = \gcd(r', s') = \gcd(r'', s'')$. Then $g'|(r/2)$, $g'|(s/2)$, and $g = 2g'$ follows by Lemma 2.2. □

Proposition 2.5. *The bottom $B(O)$ of an orbit O is either a single point or a directed cycle. Moreover, $B(O)$ is a singleton if and only if $(r, r) \in O$ for some r, in which case $B(O) = \{(r, r)\}$.*

Proof: Let $B = B(O)$. If $(r, r) \in O$ then $B = \{(r, r)\}$ because $r = \gcd(r, r) > \gcd(a, b)$ for any $(a, b) \in O$ with $a \neq b$ (since either $a < r$ or $b < r$).

Assume that $(r, r) \notin O$. Let $v \in B$. Then Lemma 2.2 implies $\omega(v) \in B$. By induction, $C = \{\omega^k(v);\ k \geq 0\} \subseteq B$. By finiteness, there is a least $t > 0$ such that $\omega^t(v) = \omega^k(v)$ for some $0 \leq k < t$. If $k > 0$ then $\omega^k(v)$ has two distinct ω-preimages, $\omega^{k-1}(v)$ and $\omega^{t-1}(v)$, both at the same depth, which contradicts Lemma 2.4. Hence $k = 0$ and C is a directed cycle.

Suppose there is $v' \in B \setminus C$, and let $C' = \{\omega^k(v');\ k \geq 0\}$ be the directed cycle determined by v'. By Lemma 2.1, there are $m, n \in \mathbb{N}$ such that $\omega^m(v) = \omega^n(v') = v''$. Then $v'' \in C \cap C'$, and $v' \in C$ follows, a contradiction. □

Let us call a rooted tree T an *extended complete binary tree* if T is rooted at r and consists of an edge rt and a complete binary tree attached to t. The *height* of a rooted tree is the length of its longest branch.

Theorem 2.6 (Shape of orbits)**.** *Every orbit $O = O(r, s)$ consists of a directed cycle $B = B(O)$, possibly degenerated into a point, to which disjoint trees are attached. If $|B| > 1$, there is one tree attached to every node of B. If $|B| = 1$, there are two trees attached to the unique node of B. Moreover:*

(i) *when $|O| > 1$, each tree attached to B is an extended complete binary tree of height a, where $\gcd(B) = 2^a b$, b odd,*
(ii) *$O = B = \{(2^k r \mod (r+s),\ 2^k s \mod (r+s));\ k \geq 0\}$ if and only if $r+s$ is odd,*
(iii) *$|O| = |B|2^a$ if $|B| > 1$, and $|O| = 2^{a+1} - 1$ if $|B| = 1$.*

Proof: We use Lemmas 2.2, 2.4 and Proposition 2.5 freely. Suppose that (r, s) is a node at even depth g. Then (r, s) has two ω-preimages. If $(r, s) \in B$ and $|B| > 1$ then exactly one of these ω-preimages is in the cycle B, while the other is at depth $g/2$. If $(r, s) \notin B$, both ω-preimages of (r, s) are at depth $g/2$. The binary tree arising in this process keeps growing until the shallowest depth b is reached, where $\gcd(B) = 2^a b$, b odd. The rest follows from the fact that a complete binary tree of height h has $1 + 2 + \cdots + 2^h = 2^{h+1} - 1$ nodes. □

Note that Theorem 2.6 implies that the shape of the orbit $O(r, s)$ is determined once the length of the bottom cycle and the highest power of 2 dividing $r + s$ are known.

In the following lemma we let $B(r, s)$ to denote the bottom of $O(r, s)$.

Lemma 2.7. *Let $r, s > 0$, and let t be a common divisor of r, s. Assume $(r, s) \in B(r, s)$. Then $(r/t, s/t) \in B(r/t, s/t)$ and $B(r, s) = t \cdot B(r/t, s/t) = \{(ta, tb);\ (a, b) \in B(r, s)\}$. When $g = \gcd(r, s)$, then $r/g + s/g$ is odd and $B(r, s) = g \cdot B(r/g, s/g) = g \cdot O(r/g, s/g)$.*

Proof: Let $r + s = 2^a b$, b odd, $g = \gcd(r, s) = 2^c d$, d odd. Then $(r, s) \in B(r, s)$ holds if and only if $a = c$, by Lemma 2.2. Hence $(r, s) \in B(r, s)$ implies $(r/t, s/t) \in B(r/t, s/t)$. We leave the verification of the equality $B(r, s) = t \cdot B(r/t, s/t)$ to the reader. Finally, $r/g + s/g$ is odd since $g = 2^a d$, d odd, and we are done by Theorem 2.6(ii). □

3. Complete orbits and well-defined powers

An orbit $O(r, s)$ is said to be *complete* if $|O(r, s)| = r + s - 1$, that is $O(r, s)$ contains all pairs (a, b) with a, $b > 0$ and $a + b = r + s$. An integer n is said to be *complete* if any (and hence all) orbits $O(r, s)$ with $r + s = n$ are complete.

Recalling the introduction, we say that x^n in the free alternative groupoid generated by x is *well-defined*, if the expression x^n is independent of parentheses. Obviously, if x^n is well-defined, then n must be complete.

For a prime p, let $\mathrm{GF}(p)$ be the field of order p. Recall that $a \in \mathrm{GF}(p)$ is a *primitive element* of $\mathrm{GF}(p)$ if it generates the multiplicative group $\mathrm{GF}(p) \setminus \{0\}$.

Proposition 3.1. *An integer $n > 0$ is complete if and only if either $n = 2^m$ or $n = p$ is an odd prime and 2 is a primitive element of* GF(p).

Proof: Assume that $n = 2^m$. Consider $(1, n-1) \in O(1, n-1) = O$. Since $\omega^{m-1}(1, n-1) = (2^{m-1}, 2^{m-1})$, we have $B(O) = \{(2^{m-1}, 2^{m-1})\}$. Then $|O| = 2^m - 1$ by Theorem 2.6(iii), showing that n is complete.

If $n = p$ is an odd prime then n is complete if and only if 2 is a primitive element of GF(p), by Theorem 2.6(ii).

Assume that n is not an odd prime and $n \neq 2^m$. Let p be an odd prime (properly) dividing n. Then $\gcd(1, n-1) = 1$ and $\gcd(p, n-p) = p$, and thus $(1, n-1)$, $(p, n-p)$ cannot be in the same orbit, by Corollary 2.3. This means that n is not complete. $\square$

Lemma 3.2. *Suppose that $n > pq$ is divisible by pq, where p, q are odd primes, not necessarily distinct. Then there are at least three distinct orbits $O(r, s)$ with $r + s = n$.*

Proof: Use the elements $(1, n-1)$, $(p, n-p)$ and $(pq, n-pq)$ with Corollary 2.3. $\square$

Lemma 3.3. *If $1 \leq n \leq 5$, the power x^n is well-defined in the free alternative groupoid generated by x.*

Proof: There is nothing to prove for $n \leq 2$. Any one of the alternative laws shows that x^3 is well-defined. We have shown in the introduction that x^4 is well-defined.

Since x^m are well-defined for every $m < 5$, to prove that x^5 is well-defined it suffices to show that for every $1 < i < 5$ some word uv with $|u| = i$ can be obtained from $x(x(x(xx)))$. Now, $x(x(x(xx))) = (xx)(x(xx)) = (xx)((xx)x) = ((xx)(xx))x = (((xx)x)x)x = ((xx)x)(xx)$ does just that. $\square$

Because 6 is not complete by Proposition 3.1, x^6 is not well-defined. However, we cannot conclude right away that x^n is not well-defined for every $n > 5$. The catch is that it could happen that the alternative laws apply to higher powers, say x^8, in so many ways that x^n could be well-defined. The following technical lemma will help us eliminate such a possibility:

Lemma 3.4. *Let u, v be words such that $|u| + |v| = n$ and $|u|$ is odd. Further assume that one of the following two conditions holds:*

(i) *n is odd and not complete,*
(ii) *n is even, n is as in Lemma 3.2, $n/2$ is odd.*

Then there is a word w of length n such that $u(uv) \neq uw$ in the free alternating groupoid A generated by x. In particular, $x^{n+|u|}$ is not well-defined in A.

Proof: Let $|u| = r$, $|v| = s$, $r + s = n$. Since n is not complete, there exists $0 < t < n$ such that $(r, s) \notin O(t, n-t)$. Should we assume (ii), we can further demand that $t \neq n/2$, by Lemma 3.2.

Let w be any word of the form w_1w_2 where $|w_1| = t$, $|w_2| = n - t$. If $u(uv) = u(w_1w_2)$, then any proof of this fact must involve some of the letters in the left-most u, because $(r, s) \notin O(t, n - t)$, and thus $uv \neq w_1w_2$. Since such a proof terminates in $u(w_1w_2)$, there is a step in the proof when the word becomes u_1u_2, $|u_1| = r$, and such that all additional steps are performed inside u_1 or u_2. We claim that such a step is either impossible, or yields u_2 that cannot be transformed to w_1w_2.

How could the word u_1u_2 be produced? Assume it is produced by the left alternative law. Then the step is either $y(yu_2) = (yy)u_2 = u_1u_2$, contradicting $|u| = |u_1|$ odd, or it is $(u_1u_1)z = u_1(u_1z) = u_1u_2$, in which case u_2 cannot be transformed to w_1w_2 because $(r, s) \notin O(t, n - t)$. Now assume that the step in question is produced by the right alternative law. When the step is $y(u_2u_2) = (yu_2)u_2 = u_1u_2$ we reach a contradiction as $|u_1| = r < |u_2| = n$. Assume the step is $(u_1z)z = u_1(zz) = u_1u_2$. This is clearly impossible when n is odd. Otherwise (ii) is assumed, and hence $t = |w_1| \neq n/2$. But $u_2 = zz$, $|z| = n/2$, $n/2$ is odd and $|O(n/2, n/2)| = 1$, so u_2 cannot be transformed into w_1w_2. □

Lemma 3.5. *The power x^n is well-defined in the free alternative groupoid generated by x if and only if $n \leq 5$, except possibly $n = 11$, $n = 13$.*

PROOF: Because 7 is not complete, Lemma 3.4 implies that x^8 is not well-defined. Let $n = 2^m > 8$, and let k be the largest odd multiple of 3 smaller than n. Note that either $n = k+1$ or $n = k+5$, and thus $k > 3$, $n < 2k$. Since k is not complete by Proposition 3.1, x^n is not well-defined by Lemma 3.4. Any even n that is not a power of 2 is not complete, by Proposition 3.1, and we have therefore shown that x^n is not well-defined for any even $n > 4$.

Now assume that $n > 5$ is odd. All odd multiples of 18 satisfy assumption (ii) of Lemma 3.4. The lemma therefore implies that x^n is not well-defined for any odd n between 18 and 36, between $3 \cdot 18 = 54$ and 108, between $5 \cdot 18 = 90$ and 180, etc. Moreover, 30 satisfies assumption (ii) of Lemma 3.4, too, and thus x^n is not well-defined for any odd n between 30 and 60. Since none of 7, 9, 15, 17 is complete, by Proposition 3.1, we are through. □

A more subtle argument (a higher dimensional dynamical system) is needed to eliminate the possibility that x^{11} or x^{13} is well-defined:

Lemma 3.6. *Let A be the free alternative groupoid generated by x. Then $x^3x^5 \neq x^4x^4$ in A. Consequently, x^{11}, x^{13} are not well-defined in A.*

PROOF: Since 3, 5 are odd, we can only transform x^3x^5 into $(x^3x^3)x^2$. Because $|O(3, 3)| = 1$, we can either return to $x^3(x^3x^2)$, or proceed to $((x^3x^3)x)x$, from which point we cannot proceed any further. The powers we have reached are of the form x^3x^5, x^6x^2, x^7x, but not x^4x^4.

Note that $(x^3x^3)x^5$ can only be transformed to $x^3(x^3x^5)$. Since $x^3x^5 \neq x^4x^4$, the expression $x^3(x^3x^5)$ can only be transformed to x^3x^8 or to $(x^3x^3)x^5$. Thus

x^{11} is not well-defined.

Similarly, $x^3(x^5x^5)$ can only be transformed to $(x^3x^5)x^5$ (because $|O(5,5)|=1$). Since $x^3x^5 \neq x^4x^4$, we conclude that x^{13} is not well-defined either. $\square$

Corollary 3.7. *The power x^n is well-defined in a free alternative groupoid generated by x if and only if $n \leq 5$.*

4. Flips

For $r, s > 0$, we say that (r,s) *flips* if $(s,r) \in O(r,s)$. Whether or not the element $(1,r)$ flips is related to the existence of two-sided inverses in alternative loops. We explain this in more detail in the next section. For the time being, we can think of flipping as a concept related to well-defined powers.

Clearly, if $r+s$ is complete or if $r = s$ then (r,s) flips. We first investigate flips for $r+s$ odd. The situation is more transparent in the odd case then in the even case thanks to Theorem 2.6(ii). The even case is handled by Proposition 4.10.

The suspected connection to number theory reveals itself in the following result:

Proposition 4.1. *Assume that $r, s > 0$ and $r+s$ is odd. Then (r,s) flips if and only if there is $k \geq 0$ such that $2^k r \equiv -r \pmod{r+s}$. If further $\gcd(r,s) = 1$, then (r,s) flips if and only if there is $k \geq 0$ such that $2^k \equiv -1 \pmod{r+s}$.*

Proof: All congruences in this proof are modulo $r+s$. By Theorem 2.6(ii), (r,s) flips if and only if there is $k \geq 0$ such that $s \equiv 2^k r$, $r \equiv 2^k s$. Since $r+s \equiv 2^k(r+s)$, we see that the above two congruences hold if and only if at least one of them holds, say $s \equiv 2^k r$. As $s \equiv -r$, (r,s) flips if and only if $2^k r \equiv -r$.

Assume that $\gcd(r,s) = 1$. Then $\gcd(r, r+s) = 1$, too, and the last congruence is therefore equivalent to $2^k \equiv -1$. $\square$

When $\gcd(r,s) \neq 1$, the situation can be reduced to the relatively prime case (see Proposition 4.10). We are thus interested in solutions k to the congruence

$$2^k \equiv -1 \pmod{n}. \tag{1}$$

Of course, (1) has no solution when n is even. When n is odd, the behavior of (1) appears to be a difficult number theoretic question, related to the classical problem whether 2 is a primitive element modulo n. We do not fully understand for which values of n the congruence (1) has a solution. Nevertheless, based on the prime factorization of n, we can identify many values of n for which there is no solution, and others for which there is a solution.

Lemma 4.2. *Suppose p is an odd prime. The congruence $2^k \equiv -1 \pmod{p}$ has a solution if and only if the multiplicative order of 2 in $\mathrm{GF}(p)$ is even.*

Proof: All congruences in this proof are modulo p. Assume that the order of 2 is an odd number m and that $2^k \equiv -1 \pmod{p}$. Then we have a contradiction via $1 \equiv 1^k \equiv (2^m)^k \equiv \left(2^k\right)^m \equiv (-1)^m \equiv -1$.

On the other hand, if the order of 2 is an even number m, then we have $2^m - 1 \equiv \left(2^{m/2} - 1\right)\left(2^{m/2} + 1\right) \equiv 0$, which implies $2^{m/2} \equiv 1$ or $2^{m/2} \equiv -1$, the former contradicting the fact that 2 is of order m. □

Many of our results are based on quadratic residues. We recall some of the relevant definitions and results from elementary number theory. (See [1].)

Let p be an odd prime and $\gcd(a, p) = 1$. Then a is said to be a *quadratic residue modulo p* if the congruence $x^2 \equiv a \pmod{p}$ has a solution. The *Legendre symbol* (a/p) is then defined by

$$(a/p) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p, \\ -1, & \text{otherwise.} \end{cases}$$

Lemma 4.3 (Euler's Criterion). *Let p be an odd prime and* $\gcd(a, p) = 1$. *Then*

$$(a/p) = a^{(p-1)/2} \mod p.$$

Lemma 4.4. *Assume that p is an odd prime. Then*

$$(2/p) = \begin{cases} 1, & \textit{if } \ p \equiv 1 \pmod{8} \ \textit{ or } \ p \equiv 7 \pmod{8}, \\ -1, & \textit{if } \ p \equiv 3 \pmod{8} \ \textit{ or } \ p \equiv 5 \pmod{8}. \end{cases}$$

In particular, the following proposition now follows easily:

Proposition 4.5. *Let p be an odd prime, and let $r, s > 0$ be such that $r + s = p$,* $\gcd(r, s) = 1$. *Then:*

(i) *if $p \equiv 3$ or $5 \pmod{8}$ then (r, s) flips,*
(ii) *if $p \equiv 7 \pmod{8}$ then (r, s) does not flip.*

Proof: Assume $p \equiv 3$ or $5 \pmod{8}$. Then $2^{(p-1)/2} \equiv -1 \pmod{p}$, so (1) has a solution, and (i) follows.

To see (ii), note that if $p \equiv 7 \pmod{8}$ then $2^{(p-1)/2} \equiv 1 \pmod{p}$. Hence the order of 2 in $GF(p)$ divides $(p-1)/2$, which is odd. Then (1) has no solution by Lemma 4.2. □

Theorem 4.6 (Chinese Remainder Theorem). *Let $n_1, \dots, n_m$ be pairwise relatively prime integers, and let $a_1, \dots, a_m$ be integers. Then there exists a unique solution x of the system of congruences $x \equiv a_i \pmod{n_i}$ with $0 \le x < n_1 n_2 \cdots n_m$.*

Lemma 4.7. *Let n be odd, and let $r, s > 0$ be such that $r + s = n$ and* $\gcd(r, s) = 1$. *Then the following conditions are equivalent:*

(i) *(r, s) flips,*
(ii) *there is $a \in \mathbb{N}$ such that for every prime p dividing n there is k_p satisfying $2^{k_p} \equiv -1 \pmod{p}$ such that $k_p = 2^a b_p$, b_p odd,*
(iii) *there is $a \in \mathbb{N}$ such that for every prime p dividing n there is k_p satisfying $2^{k_p} \equiv -1 \pmod{p}$, and every such solution satisfies $k_p = 2^a b_p$ for some odd b_p.*

PROOF: We first show the equivalence of (i) and (ii).

Assume that (i) holds. Then $2^k \equiv -1 \pmod{n}$ for some k. Thus $2^k \equiv -1 \pmod{p}$ for every prime divisor p of n, and it suffices to set $k_p = k$.

Conversely, assume (ii), let $n = p_1^{m_1} \cdots p_\ell^{m_\ell}$ be the prime factorization of n, and let $k_i = 2^a b_i$ be such that b_i is odd and $2^{k_i} \equiv -1 \pmod{p_i}$ for every i. We first show by induction on r that $2^{kp^{r-1}} \equiv -1 \pmod{p^r}$ holds for every $k = k_i$, $p = p_i$ and $r > 0$. There is nothing to prove for $r = 1$. Let $x = 2^{kp^{r-1}}$ and assume that $x \equiv -1 \pmod{p^r}$. Since p is odd, we have $x^p + 1 = (x+1)\sum_{i=0}^{p-1}(-1)^i x^i$. By the induction hypothesis, p^r divides $x+1$. Then $x \equiv -1 \pmod{p}$, too, and thus $\sum_{i=0}^{p-1}(-1)^i x^i \equiv \sum_{i=0}^{p-1}(-1)^i(-1)^i \equiv p \equiv 0 \pmod{p}$. Altogether, p^{r+1} divides $x^p + 1$, and the claim is proved. Now let $K = 2^a(b_1 p_1^{m_1-1} \cdots b_\ell p_\ell^{m_\ell-1})$. By the claim, $2^{k_i p_i^{m_i-1}} \equiv -1 \pmod{p_i^{m_i}}$. As $k_i = 2^a b_i$, K is an odd multiple of $k_i p_i^{m_i-1}$, and so $2^K \equiv -1 \pmod{p_i^{m_i}}$. Then $2^K \equiv -1 \pmod{n}$ by the Chinese Remainder Theorem, and (r, s) flips.

Condition (iii) implies (ii). To see the converse, it suffices to show that any two solutions to $2^k \equiv -1 \pmod{p}$ are divisible by the same powers of 2. Assume that $2^u \equiv -1 \equiv 2^v \pmod{p}$, $u = 2^a b$, b odd, $v = 2^c d$, d odd, and that $a > c$. Then $-1 \equiv (-1)^d \equiv (2^u)^d \equiv 2^{2^a bd} \equiv 2^{2^c d b 2^{a-c}} \equiv (2^v)^{b2^{a-c}} \equiv (-1)^{b2^{a-c}} \equiv 1$, a contradiction. □

Theorem 4.8. *Let n be odd, and let $r, s > 0$ be such that $r + s = n$ and* $\gcd(r, s) = 1$. *Then:*

(i) *if every prime p dividing n satisfies $p \equiv 3 \pmod{8}$ then (r, s) flips,*
(ii) *if every prime p dividing n satisfies $p \equiv 5 \pmod{8}$ then (r, s) flips,*
(iii) *if n is divisible by primes $p \equiv 3$, $q \equiv 5 \pmod{8}$ then (r, s) does not flip,*
(iv) *if n is divisible by a prime p with $p \equiv 7 \pmod{8}$ then (r, s) does not flip.*

PROOF: For a prime divisor p of n, let $k_p = (p-1)/2$. When $p \equiv 3 \pmod{8}$ then k_p is odd and $2^{k_p} \equiv -1 \pmod{p}$. When $p \equiv 5 \pmod{8}$ then k_p is even, not divisible by 4, and $2^{k_p} \equiv -1 \pmod{p}$. Parts (i), (ii) and (iii) therefore follow by Lemma 7.7. When $p \equiv 7 \pmod{8}$ then $2^k \equiv -1 \pmod{p}$ has no solution, as explained in the proof of Proposition 4.5, and (iv) follows again by Lemma 4.7. □

Remark 4.9. The cases not covered in Theorem 4.8 seem to be complicated. For instance:

$17 \equiv 1 \pmod{8}$ and $(1, 16)$ flips,
$73 \equiv 1 \pmod{8}$ and $(1, 72)$ does not flip,
$51 = 17 \cdot 3 \equiv 1 \cdot 3 \pmod{8}$, and $(1, 50)$ does not flip,
$843 = 281 \cdot 3 \equiv 1 \cdot 3 \pmod{8}$, and $(1, 842)$ flips,
$85 = 17.5 \equiv 1 \cdot 5 \pmod{8}$, and $(1, 84)$ does not flip,
$205 = 41 \cdot 5 \equiv 1 \cdot 5 \pmod{8}$, and $(1, 204)$ flips.

In order to fully understand such situations, we would have to know not only whether (1) has a solution k for $n = p \equiv 1 \pmod 8$, but also the highest power of 2 dividing the solution (and hence all solutions).

The following proposition tells us how to proceed in the even case or when $\gcd(r, s) \neq 1$:

Proposition 4.10. *Let $r, s > 0$, $r + s = n = 2^a b$, b odd, $\gcd(r, s) = 2^c d$, d odd, $(r', s') = \omega^{a-c}(r, s)$, $g' = \gcd(r', s')$. Then $r'/g' + s'/g'$ is odd, and (r, s) flips if and only if $(r'/g', s'/g')$ flips.*

Proof: The point (r', s') is the first point at the bottom $B = B(r, s)$ encountered along the unique directed path from (r, s), by Theorem 2.6. By Lemma 2.7, $B = g' \cdot B(r'/g', s'/g')$ and $r'/g' + s'/g'$ is odd. The rest follows. □

We conclude this section with an example:

Example 4.11. Does $(r, s) = (435, 137)$ flip? Since $435 + 137 = 572 = 2^2 \cdot 143$ and $\gcd(435, 137) = 1$, we look at $(r', s') = \omega^2(r, s) = (4 \cdot 435 \mod 572, 4 \cdot 147 \mod 572) = (24, 548)$. Since $g' = \gcd(24, 548) = 4$, we know by Proposition 4.10 that (r, s) flips if and only if $(24/4, 548/4) = (6, 137)$ flips. The odd sum $6 + 137 = 143$ factors as $143 = 11 \cdot 13$. Since $11 \equiv 3 \pmod 8$ and $13 \equiv 5 \pmod 8$, Theorem 4.8 tells us that $(6, 137)$ does not flip. Hence $(435, 137)$ does not flip.

5. Flips and alternative loops

A groupoid with neutral element in which the equation $ab = c$ has a unique solution whenever two of the element a, b, c are given is known as a *loop*. In particular, we can cancel on the left and on the right in a loop, i.e., $xy = xz$ or $yx = zx$ implies $y = z$. Multiplication tables of finite loops are therefore precisely normalized Latin squares. See [5] for an introductory text on the theory of loops.

Let L be a loop with neutral element e. Then for every $x \in L$ there are uniquely determined y, $z \in L$ such that $xy = zx = e$. If $y = z$, we say that x has a *two-sided inverse*.

A loop is *alternative* if it satisfies the left and right alternative laws. Although it is trivial to construct finite loops without two-sided inverses, no finite alternative loops without two-sided inverses are known.

Problem (Warren D. Smith (2004))**.** *Is there a finite alternative loop without two-sided inverses?*

To see the connection between this problem and flips, consider the following:

Assume that L is a finite loop, and let $x \in L$. Define the left powers $x^{(n)}$ recursively by $x^{(0)} = e$, $x^{(n+1)} = xx^{(n)}$. Let $x^{[n]}$ denote the analogously defined right powers.

By finiteness of L, there is a smallest positive integer n such that $x^{(n)} = x^{(m)}$ for some $0 \leq m < n$. If $m > 0$ then $xx^{(n-1)} = x^{(n)} = x^{(m)} = xx^{(m-1)}$, and the left cancelation implies that $x^{(n-1)} = x^{(m-1)}$, a contradiction with the minimality of n.

Thus for every x there exists n such that $xx^{(n)} = e$. Similarly, there exists m such that $x^{[m]}x = e$. Clearly then, x has a two-sided inverse if and only if $x^{(n)} = x^{[m]}$ for the above integers n, m.

Assume that $xx^{(n)} = e$. If it were possible to conclude that $x^{(n)}x = e$ by using alternative laws only, then $(1, n)$ would have to flip. However, we know that $(1, n)$ does not flip for all values of n.

Thus any proof of Problem 5.1 must involve either cancelation or the neutral element e. For instance, one could prove $xx^{(n)} = x^{[m]}x$ by showing $v(xx^{(n)}) = v(x^{[m]}x)$ for some word v, and then canceling v. As we are going to show in the next section, the finiteness of the loop in question must also be incorporated into any such proof.

We conclude this section with an existence result of arbitrarily long intervals $(r, 1)$, …, (r, s) where no (r, i) flips.

Theorem 5.2 (Dirichlet). *Let a, b be relatively prime integers. Then the arithmetic progression $an + b$ contains infinitely many primes.*

Lemma 5.3. *Let $r, s, t > 0$ be such that t is odd, divides $r + s$, and does not divide r. If there is a directed path in $O(r, s)$ from (r, s) to (r', s'), then there is a directed path from $(r \mod t,\ s \mod t)$ to $(r' \mod t,\ s' \mod t)$ in $O(r \mod t,\ s \mod t)$.*

Proof: Since t divides $r + s$ and t does not divide r, we see that $(r \mod t) + (s \mod t) = t$.

The first coordinate of $\omega(r, s)$ is $2r \mod (r + s)$. The first coordinate of $\omega(r \bmod t,\ s \bmod t)$ is $[2(r \bmod t)] \bmod (r \bmod t + s \bmod t) = 2(r \bmod t) \bmod t = 2r \bmod t$. Thus the first coordinate of $\omega(r, s)$ is mapped onto the first coordinate of $\omega(r \mod t,\ s \mod t)$ under the map $u \mapsto u \mod t$. Since the sum of coordinates is preserved under ω, an analogous statement holds for the second coordinate.

Note that t divides $(2r \mod (r + s)) + (2s \mod (r + s)) = r + s$. Thus, if we show that t does not divide $2r \mod (r + s)$, we can repeat the step in the previous paragraph as many times as we wish; hence finishing the proof. Now, $(2r \mod (r + s)) \mod t = 2r \mod t \neq 0$ since t is odd and does not divide r. □

Proposition 5.4. *Let M be a positive integer. Then there exists $r > 0$ such that none of $(r, 1)$, $(r, 2), \dots, (r, M)$ flips.*

Proof: By Theorem 5.2, there are infinitely many primes congruent to 7 modulo 8. Let $p_1 < p_2 < \cdots < p_M$ be among such primes, and assume further that $M < p_1$. Since $p_1, p_2, \dots, p_M$ are pairwise relatively prime, there is a solution $r > 0$ to the system of congruences $r + s \equiv 0 \pmod{p_s}$, $1 \leq s \leq M$. We claim that none of $(r, 1), \dots, (r, M)$ flips.

Let $1 \leq s \leq M$, $r+s = 2^a b$, b odd. Since p_s is odd and divides $r+s = 2^a b$, p_s must divide b. But $s \leq M < p_1 \leq p_s$, and hence b cannot divide s. Thus $(r \mod b) + (s \mod b) = b$. By Theorem 4.8(iv), $(r \mod b,\ s \mod b)$ does not flip. By Lemma 5.3, (r, s) does not flip. $\square$

6. An infinite alternative loop without two-sided inverses

It is essential to include the word "finite" in the statement of Problem 5.1, as there are infinite alternative loops without two-sided inverses. The existence of such a loop was suggested by J.D. Phillips, and it was constructed for the first time by Warren D. Smith.

When our construction below is used with the parameters $S = \{a_0 = 1, a_1\}$, it yields Smith's loop. Our contribution should be regarded as a straightforward generalization of Smith's idea. We split it into several steps:

Let S_0, S_1 be cyclic subgroups of an abelian group $S = (S, \cdot, 1)$, with generators s_0, s_1, respectively. Assume that $s_0 \neq s_1$. Let x_0, x_1 be symbols. Set $L = \{a x_i^n;\ a \in S,\ i \in \{0,1\},\ n \in \mathbb{N}\}$ and identify x_i^0 with 1. Define multiplication $\circ$ on L by

$$a x_i^n \circ b x_j^m = \begin{cases} (ab) x_i^{n+m}, & i = j, \\ (ab s_i^n) x_j^{m-n}, & i \neq j,\ n \leq m, \\ (ab s_i^m) x_i^{n-m}, & i \neq j,\ n \geq m. \end{cases} \tag{2}$$

Note that the two bottom branches yield the same result when $n = m$, namely $ab s_i^n$.

Lemma 6.1. *$(L, \circ)$ defined by (2) satisfies:*

(i) *L is closed under $\circ$,*
(ii) *$a \circ b = ab$ for $a, b \in S$, and thus $S \leq L$,*
(iii) *$a \in S$ commutes and associates with every element of L.*

PROOF: Parts (i), (ii) are straightforward. We have $a \circ b x_j^m = (ab) x_j^m = (ba) x_j^m = b x_j^m \circ a$ for $a, b \in S$, $m \in \mathbb{N}$. To show that $a \in S$ associates with all elements of L, it suffices to show that $(a \circ b x_i^n) \circ c x_j^m = a \circ (b x_i^n \circ c x_j^m)$ and $(b x_i^n \circ c x_j^m) \circ a = b x_i^n \circ (c x_j^m \circ a)$ for every $b, c \in S$, $n, m \in \mathbb{N}$. Assume $n \leq m$. Then $(a \circ b x_i^n) \circ c x_j^m = (ab) x_i^n \circ c x_j^m = (abc s_i^n) x_j^{m-n} = a \circ (bc s_i^n) x_j^{m-n} = a \circ (b x_i^n \circ c x_j^m)$. Assume $n \geq m$. Then $(a \circ b x_i^n) \circ c x_j^m = (ab) x_i^n \circ c x_j^m = (abc s_i^m) x_i^{n-m} = a \circ (bc s_i^m) x_i^{n-m} = a \circ (b x_i^n \circ c x_j^m)$. The other equality is proved similarly. $\square$

Lemma 6.2. *$(L, \circ)$ is a loop without two-sided inverses.*

PROOF: We need to show that $x \circ y = z$ has a unique solution in L whenever two of the elements x, y, z are given. We prove this when x and z are given, the other case being analogous.

Let $x = ax_i^n$, $z = bx_j^m$. When $i = j$ and $n \le m$, we have $x \circ (a^{-1}b)x_i^{m-n} = z$. When $i = j$ and $n \ge m$, we let $k \ne i$ and have $ax_i^n \circ (a^{-1}bs_i^{-(n-m)})x_k^{n-m} = (aa^{-1}bs_i^{-(n-m)}s_i^{n-m})x_i^{n-(n-m)} = z$. When $i \ne j$, we have $ax_i^n \circ (a^{-1}bs_i^{-n})x_j^{m+n} = (aa^{-1}bs_i^{-n}s_i^n)x_j^{(m+n)-n} = z$. It is not hard to see that the above solutions are unique in all cases.

Now, $x_0 \circ s_0^{-1}x_1 = s_0^{-1}s_0 = 1$ and $s_1^{-1}x_1 \circ x_0 = s_1^{-1}s_1 = 1$ together with $s_0 \ne s_1$ implies that $x_0 \in L$ does not have a two-sided inverse. □

Theorem 6.3. *$(L, \circ)$ is an alternative loop without two-sided inverses.*

Proof: It remains to show that the alternative laws hold in L. We only prove the left alternative law, the right alternative law being analogous.

Let $a, b \in S$, $n, m \in \mathbb{N}$, $i \ne j$. Then

$$(ax_i^n \circ ax_i^n) \circ bx_j^m = a^2x_i^{2n} \circ bx_j^m = \begin{cases} (a^2bs_i^{2n})x_j^{m-2n}, & 2n \le m, \\ (a^2bs_i^m)x_i^{2n-m}, & 2n \ge m. \end{cases}$$

On the other hand, when $n \le m$ we have

$$ax_i^n \circ (ax_i^n \circ bx_j^m) = ax_i^n \circ (abs_i^n)x_j^{m-n} = \begin{cases} (a^2bs_i^ns_i^n)x_j^{m-2n}, & 2n \le m, \\ (a^2bs_i^ns_i^{m-n})x_i^{2n-m}, & 2n \ge m, \end{cases}$$

and when $n \ge m$ we have

$$ax_i^n \circ (ax_i^n \circ bx_j^m) = ax_i^n \circ (abs_i^m)x_i^{n-m} = (a^2bs_i^m)x_i^{2n-m}.$$

Careful comparison of cases then shows that the left alternative law holds.

When $i = j$, the left alternative law obviously holds. □

Note that all powers x^n with $n > 0$ are well defined in the loop (2).

Acknowledgment. The second author worked briefly on Problem 5.1 with J.D. Phillips and Warren D. Smith. Consequent work of Smith resulted in an unpublished manuscript [6]. The maps α, β, γ, δ of Section 1 are discussed in [6], and results concerning mirrorable integers and primes are obtained there. (An integer n is *mirrorable* if the left power $x^{(n)}$ is equal to the right power $x^{[n]}$. Therefore, if n is mirrorable then $(1, n-1)$ flips, but not necessarily vice versa.) All results of Sections 2, 3 and 4 are new, to our knowledge.

References

[1] Burton D.M., *Elementary Number Theory*, third edition, Wm. C. Brown Publishers, 1994.

[2] Dehornoy P., *The structure group for the associative identity*, J. Pure Appl. Algebra **111** (1996), 59–82.

[3] Dehornoy P., *Braids and Self-Distributivity*, Progress in Mathematics **192**, Birkhäuser, Basel, 2000.
[4] Dehornoy P., *The fine structure of LD-equivalence*, Adv. Math. **155** (2000), 264–316.
[5] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics **7**, Heldermann, Berlin, 1990.
[6] Smith W.D., *Inclusions among diassociativity-related loop properties*, preprint.
[7] van Lint J.H., Wilson R.M., *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.
[8] Wirsching G.J., *The dynamical system generated by the* $3n+1$ *function*, Lecture Notes in Mathematics **1681**, Springer, Berlin, 1998.

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208, U.S.A.

E-mail: normes@math.du.edu
petr@math.du.edu

(*Received* September 6, 2005)