A dualizable, finitely based, nilpotent loop

Eran Crockett

1 Intro

Consider the abelian groups $\mathbf{Z}_2 = (\{0,1\},+), \mathbf{Z}_3 = (\{0,1,2\},+)$. Let $T : Z_3^2 \to Z_2$ be defined by

$$T(b_1, b_2) = \begin{cases} 1 & \text{if } (b_1, b_2) = (1,2) \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathbf{L} = (Z_2 \times Z_3, \oplus)$ where $(q_1, b_1) \oplus (q_2, b_2) = (q_1 + q_2 + T(b_1, b_2), b_1 + b_2)$.

Proposition 1. *The algebra* $\mathbf{L}$ *is a nonabelian loop of nilpotence class 2. The center,* ζ*, is the kernel of the projection onto* $\mathbf{Z}_3$*.*

Proof. That $\mathbf{L}$ is a loop is trivial to prove. The remaining facts follow from [3]. □

Note that $\mathbf{L}$ is not the product of prime power order loops. Since $\mathbf{L}$ has finite signature, this implies that $\mathbf{L}$ is not supernilpotent [1]. Hence, the non-dualizability result of Bentz and Mayr [2] and the finite basis results of Vaughan-Lee[4]/Freese and McKenzie [3] do not apply. We show $\mathbf{L}$ is both dualizable and finitely-based.

2 Dualizability

Let $\mathbf{A}$ be a finite algebra. A subset D of a finite power A^k of A is called *term-closed* if there are $f_i, g_i \in \mathrm{Clo}_k(\mathbf{A}), i \in I$, such that

$$D = \{\vec{x} \in A^k : f_i(\vec{x}) = g_i(\vec{x}) \text{ for all } i \in I\}.$$

Theorem 1 ([5])**.** *Let* $\mathbf{A}$ *be a finite algebra. If there is a finite set* $\mathcal{R}$ *of compatible relations on* $\mathbf{A}$ *such that for every term-closed subset* D *of a finite power of* A *and every function* $f : D \to A$*, the following two conditions are equivalent, then* $\mathbf{A}$ *is dualizable.*

1. *f preserves every relation in $\mathcal{R}$.*
2. *f can be extended to a term operation.*

Denote $(0,0) \in L$ by 0 and $(0,0,\dots,0) \in L^k$ by $\vec{0}$. For $x \in L, \lambda \in Z_3^k, \vec{x} \in L^k$, define the following term operations:

$$0 \cdot x = 0, \qquad 1 \cdot x = x, \qquad 2 \cdot x = x \oplus x, \qquad 3 \cdot x = (x \oplus x) \oplus x$$

$$r(x) = x \oplus (x \oplus (x \oplus (x \oplus x))), \qquad \ell(x) = (((x \oplus x) \oplus x) \oplus x) \oplus x$$

$$\lambda \cdot \vec{x} = (\dots(\lambda_1 \cdot x_1 \oplus \lambda_2 \cdot x_2) \oplus \dots) \oplus \lambda_k \cdot x_k$$

$$c_\lambda(\vec{x}) = 3 \cdot (2 \cdot (\lambda \cdot \vec{x}))$$

The proof of the following proposition is left to the reader.

Proposition 2.

1. *$x \oplus r(x) = 0$ for all $x \in L$*
2. *$\ell(x) \oplus x = 0$ for all $x \in L$*
3. *$3 \cdot x \;\zeta\; 0$ for all $x \in L$*
4. *$c_\lambda(\vec{x}) \;\zeta\; 0$ for all $\lambda \in Z_3^k, \vec{x} \in L^k$*
5. *if $\vec{x} \;\zeta^k\; \vec{y}$, then $c_\lambda(\vec{x}) = c_\lambda(\vec{y})$*

We now describe the clone of term operations. In order to do so, we describe some subpowers of **L**:

$$O = \{0\}, \qquad P_0 = \{(x, y, z) \in L^3 : y \;\zeta\; 0, x \oplus y = z\}, \qquad P_1 = \{(x, y, z) \in L^3 : x \oplus y \;\zeta\; z\}$$

Proposition 3. *If $f \in \mathrm{Clo}_k(\mathbf{L})$, then*

$$f(\vec{x}) = \lambda_f \cdot \vec{x} \oplus \sum_{i \in I_f} 3 \cdot x_i \oplus \sum_{\gamma \in \Gamma_f} c_\gamma(\vec{x})$$

for some $\lambda \in Z_3^k, I_f \subseteq [k], \Gamma_f \subseteq Z_3^k - \{\vec{0}\}$. Moreover, this representation is unique, i.e. if $f = g$, then $(\lambda_f, I_f, \Gamma_f) = (\lambda_g, I_g, \Gamma_g)$.

Proof. Let $\mathcal{R} = \{O, P_0, P_1, \zeta\}$. We show

$$3^k \cdot 2^{k+3^k-1} \overset{1}{\leq} |\mathrm{Clo}_k(\mathbf{L})| \overset{2}{\leq} |\mathrm{Pol}_k(\mathcal{R})| \overset{3}{\leq} 3^k \cdot 2^{k+3^k-1}.$$

To show $\overset{1}{\leq}$, it is enough to show each representation is unique. Suppose $f = g$. By modding out by ζ, we see that $\lambda_f = \lambda_g$. Now

$$\sum_{i \in I_f} 3 \cdot x_i \oplus \sum_{\gamma \in \Gamma_f} c_\gamma(\vec{x}) = \ell(\lambda_f \cdot \vec{x}) \oplus f(\vec{x}) = \ell(\lambda_g \cdot \vec{x}) \oplus g(\vec{x}) = \sum_{i \in I_g} 3 \cdot x_i \oplus \sum_{\gamma \in \Gamma_g} c_\gamma(\vec{x}).$$

To show $I_f = I_g$ and $\Gamma_f = \Gamma_g$, we refer the reader to the appendix.

To show $\overset{2}{\leq}$, it is enough to note that each relation in $\mathcal{R}$ is a subpower.

To show $\overset{3}{\leq}$, we let f preserve $\mathcal{R}$ and show there are at most $3^k \cdot 2^{k+3^k-1}$ choices for f. The proof of this is almost identical to a proof below, so we omit it here. □

Proposition 4. *Every term closed subset D of L^k satisfies the following:*

1. *$\vec{0} \in D$*
2. *D is a union of η-classes for some $\eta \leq \zeta^k$,*
3. *if $\vec{x}, \vec{y} \in D$ and $\vec{x} \;\zeta^k\; \vec{y}$, then $\vec{x} \;\eta\; \vec{y}$,*

Proof. We may assume

$$D = \{\vec{x} \in L^k : s(\vec{x}) = 0\}$$

for some term operation $s \in \mathrm{Clo}_k(\mathbf{L})$. We may make this assumption because (right or left) subtraction is a term operation and since the intersection of subsets that satisfy the above requirements will also satisfy those requirements. Clearly, $\vec{0} \in D$.

Let $U = D \cap \vec{0}/\zeta^k$ and $\eta = \mathrm{Cg}\{(\vec{u}, \vec{0}) : \vec{u} \in U\}$. Let $\vec{x} \in D$ and suppose $\vec{x} \;\eta\; \vec{y}$. To show D is a union of η-classes, it will be enough to show $\vec{y} \in D$. First, we show U is a subalgebra of $\mathbf{L}^k$. Let $\vec{u}_1, \vec{u}_2 \in U$. Then

$$s(\vec{u}_1 \oplus \vec{u}_2) = s(\vec{u}_1) \oplus s(\vec{u}_2) = 0 + 0 = 0$$

where the first equality is due to s preserving the subpower P_0. Now, because **L** is a loop, there is $\vec{w}$ such that $\vec{y} = \vec{x} \oplus \vec{w}$ and $\vec{w} \;\eta\; \vec{0}$. So now,

$$s(\vec{y}) = s(\vec{x} \oplus \vec{w}) = s(\vec{x}) \oplus s(\vec{w}) = s(\vec{w}).$$

Since $\vec{w} \;\eta\; \vec{0}$ and $\eta = \mathrm{Cg}\{(\vec{u}, \vec{0}) : \vec{u} \in U\}$, we know $\vec{w} = t(\vec{u}_1, \ldots, \vec{u}_n, \vec{x}_1, \ldots, \vec{x}_m)$ and $\vec{0} = t(\vec{0}, \ldots, \vec{0}, \vec{x}_1, \ldots, \vec{x}_m)$ for some term operation t, elements $\vec{u}_1, \ldots, \vec{u}_n \in U$, and $\vec{x}_1, \ldots, \vec{x}_m \in L^k$. But now, since $t(\vec{0}, \ldots, \vec{0}, \vec{x}_1, \ldots, \vec{x}_m) = t(\vec{0}, \ldots, \vec{0}, \vec{0}, \ldots, \vec{0}) = \vec{0}$ and $[\eta, 1] = 0$, by the term condition,

$$\vec{w} = t(\vec{u}_1, \ldots, \vec{u}_n, \vec{x}_1, \ldots, \vec{x}_m) = t(\vec{u}_1, \ldots, \vec{u}_n, \vec{0}, \ldots, \vec{0}) \in U$$

and $s(\vec{y}) = s(\vec{w}) = 0$ and $\vec{y} \in D$, as desired.

Now suppose $\vec{x}, \vec{y} \in D$ and $\vec{x} \;\zeta^k\; \vec{y}$. We show $\vec{x} \;\eta\; \vec{y}$. By the same arguments as above, there is $\vec{z}$ such that $\vec{y} = \vec{x} \oplus \vec{z}$ with $\vec{z} \;\zeta^k\; \vec{0}$. Then

$$0 = s(\vec{y}) = s(\vec{x} \oplus \vec{z}) = s(\vec{x}) \oplus s(\vec{z}) = s(\vec{z})$$

so that $\vec{z} \in D \cap \vec{0}/\zeta^k = U$, hence $\vec{z} \;\eta\; \vec{0}$ and $\vec{y} \;\eta\; \vec{x}$.

□

Proposition 5. *The loop* $\mathbf{L}$ *is dualizable.*

Proof. Let D be a term-closed subset of L^k. Let $f : D \to L$ preserve O, P_0, P_1, and ζ.

Since f preserves P_1, O, and ζ, we have that $f : D/\zeta^k \to L/\zeta$ is well-defined and can be extended to a linear transformation

$$\vec{x}/\zeta^k \mapsto \lambda_1 \cdot x_1/\zeta + \cdots + \lambda_k \cdot x_k/\zeta : L^k/\zeta^k \to L/\zeta$$

Let $g(\vec{x})$ be defined such that $f(\vec{x}) = \lambda \cdot \vec{x} \oplus g(\vec{x})$, i.e. $g(\vec{x}) = \ell(\lambda \cdot \vec{x}) \oplus f(\vec{x})$. Since g preserves P_0, $g|_U : U \to L$ is a linear transformation $\vec{x} \mapsto \kappa_1 \cdot x_1 + \cdots + \kappa_k \cdot x_k$. Since $U \subseteq \vec{0}/\zeta^k$, we can choose each $\kappa_i \in Z_2$ and replace each x_i with $3 \cdot x_i$. Let $I = \{i : \kappa_i \neq 0\}$. Now $g(\vec{u}) = \sum_{i\in I} 3 \cdot u_i$ for $\vec{u} \in U$. Let $z(\vec{x})$ be defined so that $\lambda \cdot \vec{x} \oplus \sum_{i\in I} 3 \cdot x_i \oplus z(\vec{x}) = f(\vec{x})$, i.e. $z(\vec{x}) = \ell(\lambda \cdot \vec{x} \oplus \sum_{i\in I} 3 \cdot x_i) \oplus f(\vec{x})$. In order to show z is a sum of c_λ we need to show that if $\vec{x}, \vec{y} \in D$ with $\vec{x}\ \zeta^k\ \vec{y}$, then $z(\vec{x}) = z(\vec{y})$. Let $\vec{x}, \vec{y}$ be as above. By proposition ?, we have $\vec{x}\ \eta\ \vec{y}$. There is $\vec{u} \in U$ such that $\vec{x} = \vec{y} \oplus \vec{u}$. Now $z(\vec{x}) = z(\vec{y} \oplus \vec{u}) = z(\vec{y}) \oplus z(\vec{u}) = z(\vec{y})$, as desired. Now $f(\vec{x})$ is the restriction of a term operation, and $\mathbf{L}$ is dualizable. □

3 Finite Axiomatizability

Proposition 6. *The loop* $\mathbf{L}$ *is term equivalent to an expansion of a cyclic group.*

Proof. It is left to the reader to check that

$$x \oplus y = x + y + c_1(y + y) + c_1(x) + c_1(x + y) + c_1(x + x + y) + c_1(x + x + y + y)$$

and that

$$x + y = x \oplus y + c_1(2 \cdot y) + c_1(x) + c_1(x \oplus y) + c_1(2 \cdot x \oplus y) + c_1(2 \cdot x \oplus 2 \cdot y)$$

where in the latter case c_1 is defined as above, and in the former it is defined by

$$c_1(x) = \begin{cases} (1,0) & \text{when } x\ \zeta\ (0,1) \\ (0,0) & \text{otherwise.} \end{cases}$$

Hence the algebras $(Z_2 \times Z_3, \oplus, 0)$ and $\mathbf{E} := (Z_2 \times Z_3, +, c_1, 0)$ are term equivalent. □

Proposition 7. *Let* $\mathbf{A}, \mathbf{B}$ *be finite algebras with finite signature. If* $\mathbf{A}$ *is term equivalent to* $\mathbf{B}$ *and* $\mathbf{A}$ *is finitely based, then so is* $\mathbf{B}$.

Proposition 8. *The loop* $\mathbf{L}$ *is finitely based.*

Proof. We show $\mathbf{E}$ is finitely based. Let Σ be the set of equations below:

1. $x + (y + z) \approx (x + y) + z$
2. $x + y \approx y + x$
3. $6x \approx 0$
4. $x + 0 \approx x$
5. $2c_1(x) \approx 0$
6. $c_1(x + 3y) \approx c_1(x)$
7. $c_1(x + c_1(y)) \approx c_1(x)$

- Every term operation $f \in \mathrm{Clo}_k(\mathbf{E})$ can be written in the form

$$f(\vec{x}) = \lambda_f \vec{x} + \sum_{i\in I_f} 3x_i + \sum_{\gamma\in\Gamma_f} c_1(\gamma\vec{x})$$

for some $\lambda_f \in Z_3^k, I_f \subseteq [k], \Gamma_f \subseteq Z_3^k - \{\vec{0}\}$. This form will be called the *canonical form* of f.

Proof. The proof of this claim is similar to the proof above. □

- If $f = g \in \mathrm{clo}_k(\mathbf{E})$, then $\lambda_f = \lambda_g, I_f = I_g$, and $\Gamma_f = \Gamma_g$.

  Proof. The proof of this claim is similar to the proof above. □

- Every term t can be rewritten in canonical form using only the rules in Σ.

  Proof. It is true for variable symbols x_i and the constant symbol 0. Suppose t is in canonical form. Then

$$c_1(t(\vec{x})) = c_1(\lambda_t \vec{x}) \text{ by rules } 1, 6, 7$$

  Suppose s, t are in canonical form. Then

$$s(\vec{x}) + t(\vec{x}) = \lambda \vec{x} + \sum_{i \in I} 3x_i + \sum_{\gamma \in \Gamma} c_1(\gamma \vec{x}) \text{ by rules } 1, 2, 3, 4, 5$$

□

Now let $s \approx t$ be an equation in $\mathbf{E}$. So $f_s = f_t$ where f_t, f_s are s, t rewritten in canonical form, respectively. Now $\Sigma \models s \approx f_s$ and $t \approx f_t$. Therefore $\Sigma \models s \approx t$.

□

4 Appendix

For $x = (q, b) \in L$, let $\overline{x} = q \in Z_2$. Let $i \in [k], \lambda \in Z_3^k$. Define $\vec{e}_i, \vec{w}_\lambda \in L^k$ as follows:

$$\vec{e}_i = ((0,0), \ldots, (0,0), \overset{i}{(1,0)}, (0,0), \ldots, (0,0))$$

$$\vec{w}_\lambda = ((0, \lambda_1), (0, \lambda_2), \ldots, (0, \lambda_k))$$

Let $3_i : L^k \to L$ be defined by $3_i(\vec{x}) = 3 \cdot x_i$.

Proposition 9. *The operations $3_i, c_\lambda$ for $i \in [k], \lambda \in Z_3^k$ are linearly independent in* $\mathrm{Clo}_k(\mathbf{L}) \cap (0/\zeta)^{L^k}$.

Proof. To do this it is enough to show the $(k + 3^k - 1) \times (k + 3^k - 1)$ matrix

$$Q_k = \begin{pmatrix} \overline{3_1(\vec{e}_1)} & \cdots & \overline{3_1(\vec{e}_k)} & \cdots & \overline{3_1(\vec{w}_\mu)} \\ \vdots & & \vdots & & \vdots \\ \overline{3_k(\vec{e}_1)} & \cdots & \overline{3_k(\vec{e}_k)} & \cdots & \overline{3_k(\vec{w}_\mu)} \\ \vdots & & \vdots & & \vdots \\ \overline{c_\lambda(\vec{e}_1)} & \cdots & \overline{c_\lambda(\vec{e}_k)} & \cdots & \overline{c_\lambda(\vec{w}_\mu)} \end{pmatrix}$$

is invertible. Note that $\overline{c_\lambda(\vec{e}_j)} = 0$ for all $\lambda \in Z_3^k, j \in [k]$. Also, $\overline{3_i(\vec{e}_j)} = 1$ if and only if $i = j$. So we need only show the matrix $\hat{A}_k = (\overline{c_\lambda(\vec{w}_\mu)})$ where λ, μ range over $Z_3^k - \{\vec{0}\}$ is invertible.

We define the $3^k \times 3^k$ matrices A_k, B_k, C_k as follows:

$$A_0 = \begin{pmatrix} 0 \end{pmatrix}, B_0 = \begin{pmatrix} \overline{c_1(w_1)} \end{pmatrix}, C_0 = \begin{pmatrix} \overline{c_2(w_2)} \end{pmatrix}$$

$$A_{k+1} = \begin{pmatrix} A_k & A_k & A_k \\ A_k & B_k & C_k \\ A_k & C_k & B_k \end{pmatrix}, B_{k+1} = \begin{pmatrix} B_k & B_k & B_k \\ B_k & C_k & A_k \\ B_k & A_k & C_k \end{pmatrix}, C_{k+1} = \begin{pmatrix} C_k & C_k & C_k \\ C_k & A_k & B_k \\ C_k & B_k & A_k \end{pmatrix}$$

One can show that $A_k = \begin{pmatrix} \overline{c_\lambda(\vec{w}_\mu)} \end{pmatrix}$ where the λ, μ range over Z_3^k and are ordered lexicographically. So to show $\hat{A}_k$ is invertible, it is enough to show A_k has rank equal to $3^k - 1$.

Claim: If $A_0 + B_0 = \begin{pmatrix} 1 \end{pmatrix}$, then $A_k + B_k$ is invertible for all $k \geq 0$. (The same is true if $B_0 + C_0 = \begin{pmatrix} 1 \end{pmatrix}$ or $C_0 + A_0 = \begin{pmatrix} 1 \end{pmatrix}$.)

Proof.

$$A+B = \begin{pmatrix} A+B & A+B & A+B \\ A+B & B+C & C+A \\ A+B & C+A & B+C \end{pmatrix} \rightsquigarrow \begin{pmatrix} A+B & A+B & A+B \\ A+B & B+C & C+A \\ 0 & A+B & A+B \end{pmatrix} \rightsquigarrow \begin{pmatrix} A+B & A+B & A+B \\ 0 & C+A & B+C \\ 0 & A+B & A+B \end{pmatrix} \rightsquigarrow \begin{pmatrix} A+B & 0 & A+B \\ 0 & A+B & B+C \\ 0 & 0 & A+B \end{pmatrix}$$

where each $\rightsquigarrow$ represents either an elementary row or column operation. □

Now

$$\begin{pmatrix} A & A & A \\ A & B & C \\ A & C & B \end{pmatrix} \rightsquigarrow \begin{pmatrix} A & A & A \\ 0 & A+B & C+A \\ 0 & B+C & B+C \end{pmatrix} \rightsquigarrow \begin{pmatrix} A & 0 & A \\ 0 & B+C & C+A \\ 0 & 0 & B+C \end{pmatrix}$$

Since $B_0 + C_0 = \big(1\big)$, we have $\mathrm{rk}(A_k) \geq \mathrm{rk}(A_{k-1}) + 2 \cdot \mathrm{rk}(B_{k-1} + C_{k-1}) = 3^{k-1} - 1 + 2 \cdot 3^{k-1} = 3^k - 1$.

Now A_k has rank $3^k - 1$, therefore $\hat{A}_k$ and Q_k are invertible, and the operations $3_i, c_\lambda$ are linearly independent. □

References

[1] Aichinger, Erhard; Mudrinski, Neboja. Some applications of higher commutators in Mal'cev algebras. Algebra Universalis 63 (2010), no. 4, 367403.

[2] Bentz, Wolfram; Mayr, Peter. 'Supernilpotence prevents dualizability. J. Aust. Math. Soc. 96 (2014), no. 1, 124.

[3] Freese, Ralph; McKenzie, Ralph Commutator theory for congruence modular varieties. London Mathematical Society Lecture Note Series, 125. Cambridge University Press, Cambridge, 1987.

[4] Vaughan-Lee, M. R. Nilpotence in permutable varieties. Universal algebra and lattice theory (Puebla, 1982), 293308, Lecture Notes in Math., 1004, Springer, Berlin, 1983.

[5] R. Willard. 'Four unsolved problems in congruence permutable varieties', Talk at the Conference on Order, Algebra, and Logics, Nashville, 2007.