Engel quasigroups associated with cycle systems

Sarah Zahrai*

Centre for Combinatorics, Department of Mathematics
The University of Queensland
Queensland 4072, Australia

Abstract

Many authors have studied methods of generalising Steiner quasigroups by using certain cycle systems. The usual aims have been to preserve the law $(xy)y = x$, by using the standard construction, or to preserve the law $xy = yx$, by using the opposite vertex construction. In this paper we seek to generalise the law $(xy)y = x$ to laws of the form $(\ldots(xy)y\ldots)y = x$ and $(y(\ldots(y(yx))\ldots) = x$ (reminiscent of the Engel laws which play such an important rôle in the study of Burnside groups).

1 Introduction

The quasigroups associated with certain cycle systems have been studied by many authors (see [3] for an excellent survey of this topic). The constructions used to define the quasigroup operation have been the standard construction, which preserves the law $(xy)y = x$, and the opposite vertex construction, which preserves the commutative property. In this paper we present a construction which yields quasigroups satisfying laws of the form $(\ldots(xy)y\ldots)y = x$ and $(y(\ldots(y(yx))\ldots) = x$. We call such quasigroups *right Engel* and *left Engel quasigroups* in analogy with the Engel laws in group theory.

2 Definitions and Notation

First we need the concept of a cycle system—a generalisation of Steiner triple systems.

Definition 2.1 Let K_n be the complete graph on n vertices, then a *p-cycle system of order n* is a decomposition of K_n into disjoint cycles of length p.

*This work was done while the author held a scholarship funded by the ARC. She also wishes to thank her supervisor, Dr. Sheila Williams, for her assistance during the preparation of this paper.

We shall abbreviate p-cycle system to p-CS, and if S is the set of vertices of K_n and C the set of cycles in the p-CS, we shall denote the system by (S, C).

As is well-known, neither of the constructions mentioned in the introduction yields a quasigroup for a general p-cycle system; a stronger condition is required.

Definition 2.2 Let (S, C) be a p-cycle system and let $C(j)$ denote the set of cycles obtained by taking the j-step cycles in the original system. The system (S, C) is said to be *j-perfect* if $(S, C(j))$ is also a cycle system.

(Note that this means that in a j-perfect p-cycle system, (S, C), every pair of vertices is joined by a path of length j in precisely one cycle of C.)

For the remainder of this paper, p will be an odd prime.

Definition 2.3 Let (S, C) be a p-cycle system. Define a binary operation $*_j$ on S by:

(1) $x *_j x = x$, $\forall x \in S$, and

(2) if $x \neq y$, take the unique cycle in which x is adjacent to y, and let $x *_j y = z$, where z is the j-th vertex from y going away from x in that cycle.

Then $*_j$ is called the *j-jump construction.*

Note that when there is no danger of ambiguity, we just use juxtaposition instead of $*_j$.

As we shall see in the next section, we are going to be working with systems that are both j-and $(j+1)$-perfect.

Definition 2.4 We shall call a cycle system which is both j-perfect and $(j+1)$-perfect, a *j^*-perfect system.*

Definition 2.5 Let $SR(j) = \{s_i \mid 1 \leq i \leq \frac{p-1}{2}\}$ be the set generated as follows:

$$\begin{aligned} s_1 &= 1, \text{ and} \\ s_i &= \begin{cases} s_{i-1} \times j \pmod p, & \text{if } s_{i-1} \leq \frac{p-1}{2} \\ (p - s_{i-1}) \times j \pmod p, & \text{if } s_{i-1} > \frac{p-1}{2}. \end{cases} \end{aligned}$$

Then a j^*-perfect p-cycle system (S, C) is said to be an *$SR(j)$-full j^*-perfect cycle system* if $C(s) \subseteq C$ for all $s \in SR(j)$.

If $SR(j) = \{1, 2, \cdots, \frac{p-1}{2}\}$, then $SR(j)$-full is simply called *full.*

Definition 2.6 Let $SL(j) = \{s_i \mid 1 \leq i \leq \frac{p-1}{2}\}$ be the set generated as follows:

$$\begin{aligned} s_1 &= 1, \text{ and} \\ s_i &= \begin{cases} s_{i-1} \times (j+1) \pmod p, & \text{if } s_{i-1} \leq \frac{p-1}{2} \\ (p - s_{i-1}) \times (j+1) \pmod p, & \text{if } s_{i-1} > \frac{p-1}{2}. \end{cases} \end{aligned}$$

Then a j^*-perfect p-cycle system (S, C) is said to be an *$SL(j)$-full j^*-perfect cycle system* if $C(s) \subseteq C$ for all $s \in SL(j)$.

If $SL(j) = \{1, 2, \cdots, \frac{p-1}{2}\}$, then $SL(j)$-full is simply called *full.*

Note that in both $SR(j)$-full and $SL(j)$-full systems, the calculations of the elements xy, $(xy)y$, $((xy)y)y$, $\cdots$ and $yx, y(yx), y(y(yx)), \cdots$ all yield answers in the original cycle.

Clearly $SL(j) = SR(j+1)$ for any j.

Example 2.7 Let $p = 13$, then we have the following $\frac{p-1}{2} = 6$ cycles:

(1)	0	1	2	3	4	5	6	7	8	9	10	11	12
(2)	0	2	4	6	8	10	12	1	3	5	7	9	11
(3)	0	3	6	9	12	2	5	8	11	1	4	7	10
(4)	0	4	8	12	3	7	11	2	6	10	1	5	9
(5)	0	5	10	2	7	12	4	9	1	6	11	3	8
(6)	0	6	12	5	11	4	10	3	9	2	8	1	7

When $j = 2, 6, 7, 11$ we need to use all six cycles, whereas if $j = 3, 4, 9, 10$, then we just need the three cycles (1), (3) and (4) and if $j = 5, 8$ only the two cycles (1) and (6).

Now let $j = 7$, then $S(7) = \{s_i \mid 1 \leq i \leq 6\}$ will be full. Let $x = 0$ and $y = 1$ be in $C(s_1)$. Then we have the following calculations to get the law $(\ldots(xy)y\ldots)y = x$.

$xy = 8$ in $C(s_1)$ where $s_1 = 1$,
$(xy)y = 4$ in $C(s_2)$ where $s_2 = 7$,
$((xy)y)y = 6$ in $C(s_3)$ where $s_3 = 3$,
$(((xy)y)y)y = 5$ in $C(s_4)$ where $s_4 = 8$,
$((((xy)y)y)y)y = 12$ in $C(s_5)$ where $s_5 = 9$,
$(((((xy)y)y)y)y)y = 2$ in $C(s_6)$ where $s_6 = 2$,
$((((((xy)y)y)y)y)y)y = 7$ in $C(s_1)$,
$(((((((xy)y)y)y)y)y)y)y = 11$ in $C(s_2)$,
$((((((((xy)y)y)y)y)y)y)y)y = 9$ in $C(s_3)$,
$(((((((((xy)y)y)y)y)y)y)y)y)y = 10$ in $C(s_4)$,
$((((((((((xy)y)y)y)y)y)y)y)y)y)y = 3$ in $C(s_5)$,
$(((((((((((xy)y)y)y)y)y)y)y)y)y)y)y = 0$ in $C(s_6)$.

While when $j = 4$ we have $S(4) = \{s_1, s_2, s_3\}$ and

$xy = 5$ in $C(s_1)$ where $s_1 = 1$,
$(xy)y = 11$ in $C(s_2)$ where $s_2 = 4$,
$((xy)y)y = 0$ in $C(s_3)$ where $s_3 = 3$. □

3 Preliminary results

Before stating and proving the main theorems, we need some number theory results. We thank K.R. Matthews for helpful conversations leading to the proof of the first of these.

In the following we denote the order of x modulo p by '$\mathrm{Or}(x)$'.

Lemma 3.1 *Let p be an odd prime and $p = j + r$, then*
a) either $\mathrm{Or}(j) = \frac{1}{2} \times \mathrm{Or}(r)$ *or* $\mathrm{Or}(j) = 2 \times \mathrm{Or}(r)$;
or
b) $\mathrm{Or}(j) = \mathrm{Or}(r)$ *and* $p \equiv 1 \pmod 4$
(Moreover if $p \equiv 1 \pmod 4$ *and r is a primitive root, then* $\mathrm{Or}(j) = \mathrm{Or}(r)$*).*

Proof. Let p be a prime, $\alpha = \mathrm{Or}(j)$ and $\beta = \mathrm{Or}(r) = \mathrm{Or}(-j) \pmod p$, then:
(i) $j^\alpha \equiv 1 \pmod p$, and
(ii) $(-j)^\beta \equiv 1 \pmod p$.
(i) implies $(-j)^{2\alpha} \equiv j^{2\alpha} \equiv 1 \pmod p$. Hence $\beta | 2\alpha$ and thus $2\alpha = t\beta$ for some t.
(ii) implies $1 \equiv ((-j)^\beta)^2 \equiv j^{2\beta} \pmod p$. Hence $\alpha | 2\beta$. Now these two results imply $t\beta | 4\beta$. Therefore $t|4$, and so $t = 1$ or 2 or 4.

To show if $p = 4m + 3$, then $t = 2$ is impossible:
Let $t = 2$, then $\alpha = \beta$. So we have $1 \equiv (-j)^\alpha \equiv (-1)^\alpha \pmod p$. Hence $\alpha = 2s$ for some s. Also $j^{2s} \equiv 1$ and then either $j^s \equiv 1$ or $j^s \equiv -1 \pmod p$. But $s < \alpha$ so $j^s \equiv -1 \pmod p$. As $p \equiv -1 \pmod 4$, then s must be odd. Now $(-j)^s \equiv 1 \pmod p$, implies $\beta | s$ and $2s | s$, which is a contradiction.

To show if $p = 4m + 1$ and r is a primitive root, then $\mathrm{Or}(j) = \mathrm{Or}(r)$:
Let $r^{p-1} \equiv 1 \pmod p$ and $(-r)^x \equiv 1 \pmod p$. Then $1 \equiv (-r)^x \equiv (-1)^x (r)^x$. If x is even, then $r^x \equiv 1$ and hence $x = p - 1$ as $(p-1)|x$. If x is odd, then $r^x \equiv -1$, so $r^{2x} \equiv 1$ and $(p-1)|2x$ imply $2m|x$ which is a contradiction. Therefore $x = p - 1$. □

Lemma 3.2 *Let p be an odd prime and $p = j + r$, then*
a) if $\mathrm{Or}(j)$ *is even, then either* $\mathrm{Or}(r) = \frac{1}{2} \times \mathrm{Or}(j)$ *or* $\mathrm{Or}(r) = \mathrm{Or}(j)$ *and* $p \equiv 1 \pmod 4$*; and*
b) if $\mathrm{Or}(j)$ *is odd, then* $\mathrm{Or}(r) = 2 \times \mathrm{Or}(j)$.

Proof. Let $\mathrm{Or}(j) = \alpha$ and $\mathrm{Or}(r) = \beta$,
a) Let $\alpha = 2\lambda$. Then $r^\alpha \equiv (-j)^\alpha = (-j)^{2\lambda} = (-1)^{2\lambda} j^{2\lambda} = j^{2\lambda} \equiv 1$. Hence $\beta | 2\lambda$. Also $j^\beta \equiv (-r)^\beta \equiv (-1)^\beta$.

If β is even, then $j^\beta \equiv 1$ and $\alpha | \beta$ so $2\lambda | \beta$. Thus $\beta = 2\lambda = \alpha$.

If β is odd, then $j^{2\beta} \equiv (-1)^{2\beta} \equiv 1$, hence $\alpha | 2\beta$ so $2\lambda | 2\beta$ and $\lambda | \beta$. But β is odd, and $\beta | 2\lambda$ so $\beta | \lambda$. Thus $\beta = \lambda$.

Therefore if $\mathrm{Or}(j) = 2\lambda$, then $\mathrm{Or}(j) = \mathrm{Or}(r) = 2\lambda$ or $\mathrm{Or}(r) = \frac{1}{2}\mathrm{Or}(j) = \lambda$. From Lemma 3.1 the first case can happen only when $p \equiv 1 \pmod 4$.

b) Let $\mathrm{Or}(j) = \alpha = 2\lambda + 1$. Then $r^\alpha \equiv (-j)^\alpha \equiv -1$, so $r^{2\alpha} \equiv 1$ and $\beta | 2\alpha$. Hence $2\alpha = d\beta$ for some d. Also $j^\beta \equiv (-r)^\beta \equiv (-1)^\beta$.

If β is even, then $j^\beta \equiv 1$ and $\alpha | \beta$, hence $\beta = d'\alpha$, for some d'. Thus $dd' = 2$. Now we can only have $d = 1$ and $d' = 2$ or $d = 2$ and $d' = 1$. If $d = 1$ and $d' = 2$, then $\beta = 2\alpha$ as required. If $d = 2$ and $d' = 1$, then $\beta = \alpha$ which is a contradiction as β is even and α is odd.

If β is odd, then $j^{2\beta} \equiv 1$ implies that $\alpha | 2\beta$ and as α is odd $\alpha | \beta$ and therefore $\beta = d''\alpha$, for some d''. Thus $dd'' = 2$. Now if $d = 1$ and $d'' = 2$, then $\beta = 2\alpha$ which is a contradiction as β is odd. If $d = 2$ and $d'' = 1$, then $\beta = \alpha$. In this case we have $1 \equiv r^\beta \equiv r^\alpha \equiv (-j)^\alpha \equiv -1$. Hence $1 \equiv -1 \pmod p$ which will happen only if $p = 2$. So for $p > 2$, if $\mathrm{Or}(j)$ is odd, then $\mathrm{Or}(r) = 2\mathrm{Or}(j)$.

Hence for $p = j + r$ if the order of one of j or r is even, then the order of the other will be odd. □

4 Main Results

4.1 Right Engel Quasigroups

Now let us consider the conditions under which our j-jump construction yields a quasigroup. (Recall that p is an odd prime.)

Theorem 4.1 *Let (S, C) be a p-CS. Then the groupoid constructed from (S, C) using the j-jump construction is a quasigroup if and only if (S, C) is a j^*-perfect system.*

Proof. Let c be a cycle of length p and let $c(j)$, the distance j graph of c, be the graph formed by joining vertices that are distance j apart in c. Now let (S, C) be a p-cycle system of order n and set $C(j) = \{c(j) | c \in C\}$. Then if $(S, C(j))$ is an edge disjoint decomposition of K_n based on S, (S, C) is j-perfect. Now let (S, C) be j-perfect and $(j + 1)$-perfect, so $(S, C(j))$ and $(S, C(j + 1))$ are both edge disjoint decompositions of K_n based on S. Then for any pair of vertices $a, b \in S$, where $a \neq b$, there are vertices x, y, z in S such that C has p-cycles of the form

$$(a, b, x_1, x_2, \cdots, x_{j-1}, x, \cdots, x_{p-3})$$

and

$$(a, y, y_1, \cdots, y_{j-1}, b, \cdots, y_{p-3})$$

as (S, C) is $(j + 1)$-perfect and

$$(z, a, z_1, \cdots, z_{j-1}, b, \cdots, z_{p-3})$$

since (S, C) is j-perfect.
As it is j-perfect and $(j + 1)$-perfect, each pair occurs in exactly one p-cycle. So the equations $a * b = x$ and $a * y = b$ and $z * a = b$ have unique solutions.

Now let the groupoid give us a quasigroup, then $a * y = b$ guarantees a unique p-cycle in C of the form

$$(a, y, y_1, \cdots, y_{j-1}, b, \cdots, y_{p-3})$$

and thus using distance $j + 1$, another unique cycle of the form

$$(a, b, \cdots, w_{p-3})$$

in $C(j + 1)$. So $(S, C(j + 1))$ is a p-cycle system.

Also $z * a = b$ guarantees a unique p-cycle in C of the form

$$(z, a, z_1, \cdots, z_{j-1}, b, \cdots, z_{p-3})$$

and using distance j, another unique cycle of the form

$$(a, b, \cdots, t_{p-3})$$

in $C(j)$. So $(S, C(j))$ is a p-cycle system. □

We can now show that we have an Engel quasigroup. Recall that in an $SR(j)$-full and $SL(j)$-full cycle systems all iterations of $*_j$ can be performed within a single cycle (see Example 2.7).

Theorem 4.2 *Let (S, C) be an $SR(j)$-full j^*-perfect p-cycle system. Then the quasigroup constructed using the j-jump construction satisfies the following law :*

$$(\cdots((x*_j \underbrace{y)*_j y)*_j \cdots)*_j y}_{k} = x$$

where $k = \mathrm{Or}(r)$ is the order of $r = p - j \pmod p$.

Proof. The function $*_j$ on the set of vertices $\{0, 1, \cdots p-1\}$ on the cycles may also be defined by

$$x*_j y = y + (y - x) \times j = (1 + j)y + (-j)x.$$

Then

$$(x*_j y)*_j y = y + (y - (y + (y - x) \times j)) \times j = (1 - j^2)y + (-j)^2 x.$$

And at the kth stage we have

$$(\cdots((x*_j \underbrace{y)*_j y)*_j \cdots)*_j y}_{k} = (1 + (-1)^{k+1} j^k)y + (-j)^k x.$$

If $k \neq \mathrm{Or}(-j)$, then we continue the process till $k = \mathrm{Or}(-j)$. Then $(-j)^k \equiv 1 \pmod p$ and

$$(\cdots((x*_j \underbrace{y)*_j y)*_j \cdots)*_j y}_{k} = (1 + (-1)(-j)^k)y + (-j)^k x = x,$$

required. □

The following results tell us something about the number of cycles used in the calculation of the Engel laws, and the number of edges covered.

Theorem 4.3 *Let (S, C) be an $SR(j)$-full j^*-perfect p-cycle system. Then to get the law*

$$(\cdots((x*_j \underbrace{y)*_j y)*_j \cdots)*_j y}_{k} = x$$

by using the j-jump construction, where $k = \mathrm{Or}(r)$,

a) if $\mathrm{Or}(j) = 2\lambda$, then the number of cycles used is λ or 2λ when $p \equiv 1 \pmod 4$, and

b) if $\mathrm{Or}(j) = 2\lambda + 1$, then the number of cycles used is $2(2\lambda + 1)$.

Proof. Since each pair of vertices occurs in one and only one cycle, the number of cycles we use is exactly the order of r, i.e. k. Hence Lemma 3.2 gives the required results. □

Corollary 4.4 *For any p, let j be a natural number such that*
(a) j has order $\frac{p-1}{2}$; or
(b) j has order $p-1$.
Then in any $SR(j)$-full j^*-perfect p-cycle system, if p points lie on a cycle, the j distance cycles to get the law

$$(\cdots((x*_j \underbrace{y)*_j y)*_j \cdots)*_j y}_{k} = x$$

cover all of the edges between these points.

Proof. Both cases imply that $k = \mathrm{Or}(r) = p-1$ or $k = \mathrm{Or}(r) = \frac{p-1}{2}$. Using Theorem 4.3, and the fact that each pair of vertices occurs in one and only one cycle, to get the law we need to use all $\frac{p-1}{2}$ cycles. So all the edges between these p points will be used. □

Theorem 4.5 *For any p let j be a natural number such that either*
(a) j has order $p-1 \pmod p$; or
(b) j has order $\frac{p-1}{2} \pmod p$ and $p \equiv 3 \pmod 4$.
Then in any $SR(j)$-full j^*-perfect p-cycle system, if p points lie on a cycle, then the iterated distance j-cycles cover all of the edges between these points.

Proof. The conditions on p ensure that the process of iterating the construction of the distance j-cycles yields all of the edges between these p points which lie on a cycle. The extra condition in case (b) implies that -1 is not a power of j, so that all $\frac{p-1}{2}$ powers of j yield different cycles. □

Example 4.6 For instance, with $p = 23$ and $j = 4$ we get the cycles at distances $1, 4, 16 = -7, 18 = -5, 3, 12 = -11, 2, 8, 9, 13 = -10, 6$, whereas, with $p = 13$ and $j = 4$, we get only the cycles at distances $1, 4, 3, 12 = -1, 9 = -4, 10 = -3$, which does not give us all the cycles. □

4.2 Left Engel Quasigroups

In this section we exhibit some properties of left Engel quasigroups analogous to those of right Engel quasigroups.

Theorem 4.7 *Let (S, C) be an $SL(j)$-full j^*-perfect p-cycle system. Then the quasigroup constructed using the j-jump construction satisfies the following law :*

$$\underbrace{y*_j(\cdots*_j(y*_j(y}_{k}*_j x))\cdots) = x$$

where $k = \mathrm{Or}(j+1)$ is the order of $(j+1) \pmod p$.

The proof is similar to that of Theorem 4.2.

Theorem 4.8 *Let (S, C) be an $SL(j)$-full j^*-perfect p-cycle system. Then to get the law*

$$\underbrace{y*_j(\cdots *_j(y*_j(y}_{k} *_j x))\cdots) = x$$

by using the j-jump construction, where $k = \mathrm{Or}(j+1)$,

a) if $\mathrm{Or}(j+1) = 2\lambda$, then the number of cycles used is λ, and

b) if $\mathrm{Or}(j+1) = 2\lambda + 1$, then the number of cycles used is $2\lambda + 1$.

Proof. To prove the first part we show that for any two vertices x and y, after λ steps the following law will hold

$$\underbrace{y*_j(\cdots *_j(y*_j(y}_{\lambda} *_j x))\cdots) = x*_1 y,$$

which is the other vertex adjacent to y. For that, again we use the definition of $*_j$ used in 4.7.

If $k = 2\lambda = \mathrm{Or}(j+1)$, then $(1+j)^k = (1+j)^{2\lambda} = ((1+j)^\lambda)^2 \equiv 1 \pmod{p}$. Thus $(1+j)^\lambda \equiv 1$ or $(1+j)^\lambda \equiv -1$. As $\mathrm{Or}(j+1) = k$, we deduce that $(j+1)^\lambda \equiv -1$. Hence

$$\begin{aligned}
\underbrace{y*_j(\cdots *_j(y*_j(y}_{\lambda} *_j x))\cdots) &= (1+j)^\lambda x + (-1)((1+j)^\lambda - 1)y \\
&= -x + 2y \\
&= (y - x) + y \\
&= x*_1 y.
\end{aligned}$$

So after λ steps we get back to the first cycle we used, and as each pair of vertices occurs in one and only one cycle, the number of cycles we use is exactly the order of $(j+1)$, so we need to repeat the same cycles once more.

If $\mathrm{Or}(j+1) = k = 2\lambda + 1$, then trivially we need to use the same number of cycles as the order of $(j+1)$. □

Corollary 4.9 *For any prime number p, let j be a natural number such that*

a) $j+1$ has order $p-1$, or

b) $j+1$ has order $\frac{p-1}{2}$ and $p \equiv 3 \pmod 4$.

Then in any $SL(j)$-full j^*-perfect p-cycle system, if p points lie on a cycle, then the cycles used to get the law

$$\underbrace{y*_j(\cdots *_j(y*_j(y}_{\mathrm{Or}(j+1)} *_j x))\cdots) = x$$

cover all the edges between these points.

The proof is similar to that of Corollary 4.4.

5 Conclusion

One of the most interesting questions that arises in the study of quasigroups arising from cycle systems is the question of when they form varieties. Bryant and Lindner ([1]) have shown that for the standard construction applied to general 2-perfect systems, varieties are obtained only when $p = 3$, 5 or 7, whereas Bryant and Oates-Williams ([2]) have shown that, if the construction is restricted to what they call *strongly 2-perfect* systems, many more primes yield varieties. As the $SR(j)$-full and $SL(j)$-full condition we have used here closely resembles the strongly 2-perfect condition, it would be reasonable to suppose that varieties are obtained for a large number of primes. Clearly, since for example $(\cdots((x\underbrace{y)y)\cdots)y}_{6} = x$ holds for the 3-jump construction for $p = 13$, and the 5-jump construction for $p = 31$, additional laws will be required to distinguish such cases. We hope to consider these problems in a later paper.

References

[1] D.E. Bryant and C.C. Lindner, *2-perfect m-cycle systems can be equationally defined for m = 3, 5 and 7 only*, Algebra Universalis, **35** (1996), 1–7.

[2] D.E. Bryant and S. Oates-Williams, *Strongly 2-perfect cycle systems and their quasigroups*, Discrete Math, **167/168** (1997), 167–174.

[3] C. C. Lindner, *2-perfect m-cycle systems and quasigroup varieties : A Survey*, 24th annual Iranian mathematics conference, Tehran, 1993.

(Received 20/3/97)