Strong near subgroups and left gyrogroups

TOMÁS FEDER*

January 30, 2002

1 Introduction

Near subgroups of finite groups were introduced by Feder and Vardi [6] as a tool to study the computational complexity of constraint satisfaction problems. Aschbacher [2] addressed some questions raised in [6] and showed that near subgroups possess much structure. More recently, Feder [7] showed that near subgroups do indeed characterize the polynomial time solvable cases of group theoretic constraint satisfaction problems, using new structural results for near subgroups obtained by Aschbacher [3].

Near subgroups can be defined as twisted subgroups enjoying some additional properties. For odd order groups, twisted subgroups and near subgroups coincide. The order of a twisted subgroup of an odd order group divides the order of the group. More generally, the order of a twisted subgroup of an odd order group divides the order of any twisted subgroup containing it, as shown by Glauberman [9, 10].

We first consider the question of whether these results on the order of twisted subgroups apply in the case of groups that are not necessarily of odd order. We say that a twisted subgroup K of a group G is *order-dividing* in G if for every coset aH of a subgroup H of G, the order $|H|$ is divisible by $|K \cap aH|$. We introduce the notion of a *strong near subgroup* K of a finite group G, which again coincides with twisted subgroups for odd order groups. We show that if a twisted subgroup K is order-dividing in G, then K is a strong near subgroup of G. Conversely, if K is a strong near subgroup of G, then K is order-dividing in G. In fact, we generalize Glauberman's result by showing that the order of a strong near subgroup of a group divides the order of any strong near subgroup containing it. This last result depends on a characterization of strong near subgroups conjectured by this author and shown by Aschbacher [4].

Gyrogroups initially arose in the study of the Thomas precession in the special theory of relativity, and are defined by gyrogroup axioms [16, 17]. Foguel and Ungar [8] showed that every twisted subgroup of an odd order group can be viewed as a gyrocommutative gyrogroup with operation $x \oplus y = \sqrt{xy^2x}$ and gyrations $gyr[x, y]$ obtained by conjugation by $\sqrt{xy^2x}x^{-1}y^{-1}$.

This operation reminds us of the mapping used in the definition of a near subgroup. A subset K containing 1 of a finite group G is a near subgroup of G if for all a, ax, ay in K, there is an element $af_a(x, y)$ in K, where $f_a(x, y) = xyz$ with z in the commutator group of the group generated by x, y. Indeed, for odd order groups, we can set $f_a(x, y) = \sqrt{xy^2x} = x \oplus y$.

This suggests the following question. Can the operations $f_a(x, y) = xyz$ for a near subgroup always be defined so as to give a gyrocommutative gyrogroup as well? We first show that in order to have the left cancellation property of left gyrogroups hold for mappings $x \odot y = f_a(x, y)$ in $a^{-1}K$, so that the mappings are left loop operations, the near subgroup must be a strong near subgroup. We

*268 Waverley St., Palo Alto, CA 94301. E-mail: tomas@theory.stanford.edu.

then exhibit examples of strong near subgroups for which the mappings $x \odot y = f_a(x, y)$ can define left gyrogroups, but not gyrogroups (or gyrocommutative gyrogroups). This leads us to ask whether the mappings $x \odot y = f_a(x, y)$ characterizing near subgroups can always be defined in the case of strong near subgroups so as to give them a left gyrogroup structure. We exhibit special properties implying that this is the case; these properties are later generalized by Aschbacher [4], who also indicates when we may or may not expect the left gyrogroups obtained with either construction to coincide with mappings f_a characterizing near subgroups.

We finally show that the mappings $x \odot y = f_a(x, y)$ can always be defined to form a left loop satisfying the automorphic inverse property, for reduced strong near subgroups. The left loops obtained satisfying the automorphic inverse property will not in general coincide with those giving left gyrogroups.

The two parts of the paper are related by the result of Ungar [16] that every left gyrogroup can be represented as a subset B containing 1 in a group G, so that the elements of G decompose uniquely as a product of an element of B and an element of a subgroup H of G. In this representation, the order $|B|$ divides the order $|G|$ of the group.

A note about terminology. A left gyrogroup is the same as a left loop having the left inverse property (LIP) and having the A_l property. A gyrocommutative gyrogroup is the same as a Bruck loop or K-loop. A groupoid is a left loop if it has an identity and satisfies the left cancellation property. The A_l property is axioms $(G3)$ and $(G4)$ below.

2 Strong near subgroups of finite groups

The reader is directed to [1] for notation, terminology, and basic results on finite groups.

Let G be a finite group. A subset K of G is a *near subgroup* of G if $1 \in K$ and for all $b \in G$ such that $1 \in bK$, for all subgroups M of G, and for all normal subgroups N of M such that $M^* = M/N$ is abelian, the set $(bK)^* = \{aN \subseteq M : bK \cap aN \neq \emptyset\}$ is a subgroup of M^*. In brief, the intersection of K with the abelian sections of G forms subgroups.

An equivalent definition states that a subset K of G is a near subgroup of G if $1 \in K$ and for all $a \in G$ such that $1 \in a^{-1}K$, if $x, y \in a^{-1}K$, then there is an element $f_a(x, y) = xyz \in a^{-1}K$ with z in the commutator group of the group generated by $\{x, y\}$.

Of course, ordinary subgroups are near subgroups. For the purpose of our study, a different but equivalent definition is more useful. A subset K of G is a *twisted subgroup* of G if it satisfies the following two conditions:

(1) $1 \in K$.

(2) If $x, y \in K$ then $xyx \in K$.

Define a twisted subgroup K of G to be a *near subgroup* of G if it also satisfies the following condition:

(3) If N is a normal subgroup of $M \leq G$ with M/N isomorphic to E_4, then there is no $b \in G$ such that $bK \cap M$ meets exactly three of the four cosets of N in M.

The following properties of twisted and near subgroups were known in [6] and appear with proof in [2].

Lemma 1 *(1) If K is a twisted subgroup of G, then $\langle x \rangle \subseteq K$ for each $x \in K$.*

(2) If $H \leq G$ and K is a twisted subgroup (near subgroup) of G then $H \cap K$ is a twisted subgroup (resp. near subgroup) of G.

(3) If $a, b \in G$ and K is a twisted subgroup (near subgroup) of G with $1 \in aKb$, then aKb is a twisted subgroup (resp. near subgroup) of G.

(4) If N is a normal subgroup of G and K is a twisted subgroup (near subgroup) of G then K^* is a twisted subgroup (resp. near subgroup) of $G^* = G/N$.

(5) If N is a normal subgroup of G with $bN \subseteq K$ for all $b \in K$, and K^* is a twisted subgroup (near subgroup) of $G^* = G/N$, then K is a twisted subgroup (resp. near subgroup) of G.

(6) If K is a near subgroup of $G = \langle K \rangle$, and G is either abelian or a 2-group, then $G = K$.

The following is from [2]. Let K be a twisted subgroup of G such that $G = \langle K \rangle$. In $G \times G$, consider the subgroup $H_K = \langle \{(x, x^{-1}) : x \in K\} \rangle$, and let $N_K = \{x \in G : (x, 1) \in H_K\}$.

Lemma 2 *(1) N_K is a normal subgroup of G, and $bN_K \subseteq K$ for each $b \in K$.*

(2) If $N_K = 1$, then $H_K = \{(x, \tau(x)) : x \in G\}$, where $\tau = \tau_K$ is an automorphism of G with $\tau^2 = 1$, and $K \subseteq K(\tau) = \{x \in G : \tau(x) = x^{-1}\}$.

G is said to be *K-reduced* if $N_K = 1$. In general $\hat{G} = G/N_K$ is $\hat{K}$-reduced.

The *associates* of a twisted subgroup K of a group G are the twisted subgroups $a^{-1}K = Ka$ with $a \in K$.

Theorem 1 *(1) Let K be a twisted subgroup of G. Then K is a near subgroup of G if and only if for each 2-subgroup H of G, we have that $K \cap H$ is a subgroup of H.*

(2) If K is a near subgroup of G and G is K-reduced, then for each 2-subgroup H of G and each associate L of K, we have that $L \cap H$ is an abelian subgroup of H.

Proof. Part (2) is shown in [2]. The only if part of (1) follows from (6) of Lemma 1.

For the if part, let K be a twisted subgroup of G. Assume K is not a near subgroup of G, and that $G = \langle K \rangle$. Then in $G^* = G/N_K$, we have that K^* is a twisted subgroup of G^* but K^* is not a near subgroup of G^*, where G^* is K^*-reduced. It then follows from (2.7) in [2] that there is a 2-subgroup H^* of G^* such that $K^* \cap H^*$ is not a subgroup of H^*. Let H be the preimage of H^*, and let T be a Sylow 2-subgroup of H. Then $|T| = |H|_2$ and $|T \cap N_K| = |N_K|_2$, so $T^* = H^*$, and $(K \cap T)^* = K^* \cap H^*$ is not a subgroup of $H^* = T^*$. Therefore $K \cap T$ is not a subgroup of T, completing the proof. □

A near subgroup K of a finite group G is a *strong near subgroup* of G if for each $H \leq G$ and each normal subgroup N of H such that $H^* = H/N$ is a section of G isomorphic to a dihedral group D_{2q} with q odd, and for each associate L of K, it is not the case that $(L \cap H)^*$ consists precisely of the involutions plus 1 in H^*.

Theorem 2 *Let K be a near subgroup of G, where G is K-reduced. Then the following are equivalent.*

(1) K is a strong near subgroup of G.

(2) For each section $H^* = H/N$ isomorphic to a dihedral group D_{2q} with q odd, and for each associate L of K, it is not the case that $(L \cap H)^*$ consists precisely of the involutions plus 1 in H^*, N is an abelian 2-group, and $aN \subseteq L$ for each $a \in L \cap H$.

(3)The 2-elements in each associate $L = a^{-1}K = Ka$ form an abelian 2-group H_a.

For such a strong near subgroup K of G where G is K-reduced, the cosets aH_a with $a \in K$ form a partition of K and each H_a is a conjugate of H_1.

Proof. Condition (2) is a special case of the definition of a strong near subgroup, so (1) implies (2). If $M = L \cap H$, and M^* consists of the involutions in $H^* = H/N$ isomorphic to a dihedral group D_{2q} with q odd, then the 2-elements in M generate an element of odd order in H, and so the 2-elements in L do not form a 2-group. Therefore (3) implies (1).

Assume (2) holds, and let L be an associate of K. We show that the 2-elements in L commute, and so (3) holds. Suppose x, y are 2-elements in L that do not commute, with $|x| + |y|$ minimal. Then x commutes with y^2, and y commutes with x^2. Let $H = \langle x, y\rangle$, and $N = \langle x^2, y^2\rangle$, and let $M = L \cap H$. Then N is a normal subgroup of H, and x^*, y^* are involutions in $H^* = H/N = \langle x^*, y^*\rangle$, so H^* is isomorphic to a dihedral group D_{2q}. Furthermore N is an abelian 2-group with $N \subseteq M$. Since $y^* = x^*z^*$ with z^* of order q in H^*, and $x^*, y^* \in M^*$, it follows that the involutions $x^*(z^*)^i$ are in M^* as well, because M^* is a twisted subgroup of H^*. If q is even, then the involution $(z^*)^{q/2}$ is in M^* as well, because $R^* = \langle x^*, (z^*)^{q/2}\rangle$ is isomorphic to E_4 and $M^* \cap R^*$ is a near subgroup of R^* containing the three elements $1^*, x^*, x^*(z^*)^{q/2}$ and thus the fourth element $(z^*)^{q/2}$ as well. Furthermore, M^* contains only involutions plus 1^* because the automorphism τ^* on H^*, induced by the automorphism τ on G inverting L, is the identity map, since $\tau^*(x^*) = x^*$ and $\tau^*(y^*) = y^*$.

Therefore M^* consists of the involutions plus 1^* in H^*. For each such involution x^*, the group $T = \langle x\rangle N$ is a 2-group with $N \subseteq M$ and $xN \cap M \neq \emptyset$, so since $M \cap T \leq T$, we have that $T \subseteq M$. That is, M consists of the full preimages of 1^* and the involutions in H^*. This contradicts (2) if q is odd. If $q = 2r$ with r odd, then we contradict (2) again in $H^*/\langle (z^*)^r\rangle$, which is isomorphic to a dihedral group D_{2r}. If $q = 4r$, then $H' = H^*/\langle (z^*)^4\rangle$ is isomorphic to a dihedral group D_8 and M' is not a subgroup of H', which contradicts the fact that H' is a 2-group with M' as a near subgroup. Thus (2) implies (3).

If $b \in aH_a$, then $bH_b = aH_a$, so the cosets aH_a with $a \in K$ partition K. Every $a \in K$ can be written as $a = a_1a_2$ with $a_1, a_2 \in \langle a\rangle$, a_1 of odd order and a_2 a 2-element. Since $a_2 \in H_1$, we have $H_{a_2} = H_1$. Letting $K' = {a_2}^{-1}K$, we have $H'_1 = H_{a_2}$ and $H'_{a_1} = H_{a_1a_2}$. So it suffices to consider a of odd order. We then have $\sqrt{a}H_1\sqrt{a} = a((\sqrt{a})^{-1}H_1\sqrt{a}) \subseteq aH_a$, since K is a twisted subgroup of G. Containment in the reverse direction follows by a similar argument for $K'' = a^{-1}K$, so $aH_a = \sqrt{a}H_1\sqrt{a}$ for a of odd order. □

3 Order-dividing twisted subgroups

Let K be a twisted subgroup of a finite group G. Recall that the *associates* of K are the twisted subgroups $L = a^{-1}K = Ka$ for $a \in K$.

A twisted subgroup K of G is *order-dividing* in G if for each associate L of K and each subgroup H of G, the order $|H|$ is divisible by $|L \cap H|$.

Lemma 3 *If K is order-dividing in G, then K is a near subgroup of G.*

Proof. If K is not a near subgroup of G then by Theorem 1, G has a 2-subgroup H such that $L \cap H$ is not a subgroup of H for some associate $L = a^{-1}K$, and therefore also not a near subgroup of H. Choose the smallest such H. Then H has a normal subgroup N with $H^* = H/N$ isomorphic to the elementary abelian group E_4, with $L^* = \{1^*, a^*, b^*\}$ and $H^* = \{1^*, a^*, b^*, (ab)^*\}$. Also $L \cap \langle a\rangle N$ is a subgroup of $\langle a\rangle N$, so $|L \cap aN| = |L \cap N|$, and similarly $|L \cap bN| = |L \cap N|$. Therefore $|L \cap H| = 3|L \cap N|$ does not divide $|H|$. □

If G has a normal subgroup N such that the twisted subgroup K satisfies $aN \subseteq K$ for each $a \in K$, then K is order-dividing in G if and only if K^* is order-dividing in $G^* = G/N$. We shall therefore assume that G is K-reduced.

Theorem 3 *If K is order-dividing in G, then K is a strong near subgroup of G.*

Proof. By the preceding lemma, K is a near subgroup of G. If K is not a strong near subgroup of G, then with the notation of condition (2) in Theorem 2, we have $|H| = 2q|N|$ and $|L \cap H| = (q + 1)|N|$ with q odd. So $|L \cap H|$ does not divide $|H|$. □

We prove the converse of this theorem. If K is a strong near subgroup of G, and N is a normal subgroup of G, then $L \cap N$ is a strong near subgroup of N for each associate L of K, and K^* is a strong near subgroup of $G^* = G/N$.

Aschbacher [3] has obtained a complete list of near subgroups K of nonabelian finite simple groups G such that G is K-reduced; we verified with him that there are no finite simple groups G such that G is K-reduced and K is a strong near subgroup of G.

Theorem 4 *If K is a strong near subgroup of G, then K is order-dividing in G.*

Proof. The proof is by induction on $|G|$ so it suffices to show that $|K|$ divides $|G|$, and we can assume G is K-reduced. If G is simple, then by the preceding remark G is a cyclic group of prime order with $K = G$ and we are done. Otherwise G has a normal subgroup N. By inductive hypothesis, $|K \cap N|$ divides $|N|$. We show that $|K \cap aN| = |K \cap N|$ for each $a \in K$. Since $|K^*|$ divides $|G^*|$ by inductive hypothesis, we then have that $|K| = |K \cap N| \cdot |K^*|$ divides $|N| \cdot |G^*| = |G|$.

We prove the claim. It suffices to consider the cases a of odd order and a a 2-element and the group $G' = \langle a \rangle N$, because in general $a = a_1 a_2$ with a_1 of odd order and a_2 a 2-element, $a_1, a_2 \in \langle a \rangle$, so that

$$|K \cap a_1 a_2 N| = |a_1^{-1} K \cap a_2 N| = |a_1^{-1} K \cap N| = |K \cap a_1 N| = |K \cap N|.$$

If a has order $2q-1$, then $a^q (K \cap N) a^q \subseteq (K \cap aN)$ since K is a twisted subgroup of G', so $|K \cap N| \leq |K \cap aN|$. The same argument applied to a^{-1} in $L = a^{-1}K$ shows that $|K \cap aN| = |L \cap N| \leq |L \cap a^{-1}N| = |K \cap N|$, so that $|K \cap N| = |K \cap aN|$.

If a is a 2-element, then we use the fact that K is a strong near subgroup, hence by Theorem 2 partitioned into cosets bH_b, where each H_b is a conjugate of the 2-group H_1 of 2-elements in K. Since $a \in H_1$, $|H_1 \cap cN| = |H_1 \cap N|$ for each $c \in \langle a \rangle$. Therefore $|H_b \cap cN| = |H_b \cap N|$, which implies $|K \cap cN| = |K \cap N|$, and the result follows by setting $c = a$. □

The following result was conjectured by this author and shown by Aschbacher [4]. Let $O_2(G)$ denote the largest normal 2-subgroup of G.

Theorem 5 *If K is a strong near subgroup of G, and G is K-reduced, then $H_a \leq O_2(G)$ for each $a \in K$, and $G/O_2(G)$ is of odd order.*

Glauberman [9, 10] showed the following.

Theorem 6 *If G is of odd order and $L \subseteq K \subseteq G$ are twisted subgroups of G, then $|L|$ divides $|K|$.*

We generalize this result.

Theorem 7 *If $L \subseteq K \subseteq G$ are strong near subgroups of G, then $|L|$ divides $|K|$.*

Proof. Assume $\langle K \rangle = G$. Let $O'(G)$ be the smallest normal subgroup of G such that $G^* = G/O'(G)$ is of odd order. Then $|L^*|$ divides $|K^*|$ by Theorem 6. Furthermore $K \cap O'(G)$ is a subgroup of G by Theorem 5, so by Theorem 4, $|L \cap O'(G)|$ divides $|K \cap O'(G)|$. Finally $|L \cap aO'(G)| = |L \cap O'(G)|$ whenever $L \cap aO'(G) \neq \emptyset$, and $|K \cap aO'(G)| = |K \cap O'(G)|$ whenever $K \cap aO'(G) \neq \emptyset$, as in the proof of Theorem 4, so $|L| = |L^*| \cdot |L \cap O'(G)|$ divides $|K| = |K^*| \cdot |K \cap O'(G)|$. □

4 Near subgroups and gyrogroups

A groupoid $(G, \odot)$ is a *gyrogroup* if its binary operation satisfies the following axioms. In G there is at least one element, 1, called a left identity, satisfying

$$(G1) \quad 1 \odot a = a \qquad\qquad \textit{Left Identity}$$

for all $a \in G$. There is an element $1 \in G$ satisfying axiom $(G1)$ such that for each $a \in G$ there is an element a^{-1} in G, called a left inverse of a, satisfying

$$(G2) \quad a^{-1} \odot a = 1 \qquad\qquad \textit{Left Inverse}$$

Moreover, for any $a, b, z \in G$ there exists a unique element $gyr[a,b]z \in G$ such that

$$(G3) \quad a \odot (b \odot z) = (a \odot b) \odot gyr[a,b]z \qquad\qquad \textit{Left Gyroassociative Law}$$

If gyr[a,b] denotes the map $gyr[a,b] : G \to G$ mapping z to $gyr[a,b]z$ then

$$(G4) \quad gyr[a,b] \in Aut(G, \odot) \qquad\qquad \textit{Gyroautomorphism}$$

and $gyr[a,b]$ is called the Thomas gyration, or the gyroautomorphism of G, generated by $a, b \in G$. Finally, the gyroautomorphism $gyr[a,b]$ generated by any $a, b \in G$ satisfies

$$(G5) \quad gyr[a,b] = gyr[a \odot b, b] \qquad\qquad \textit{Left Loop Property}$$

Relaxing the left loop property into the weak left loop property we obtain the left gyrogroup: A groupoid $(G, \odot)$ satisfying the gyrogroup axioms $(G1)$–$(G4)$, in which the left loop property $(G5)$ is replaced with the weaker property

$$(G5') \quad gry[a, a^{-1}] = id \qquad\qquad \textit{Weak Left Loop Property}$$

is called a *left gyrogroup*, *id* being the identity map.

A gyrogroup $(G, \odot)$ is gyrocommutative if for all $a, b \in G$,

$$(G6) \quad a \odot b = gyr[a,b](b \odot a) \qquad\qquad \textit{Gyrocommutative Law}$$

Let G be a group possessing the unique decomposition $G = BH$ in the sense that every element $g \in G$ can be written uniquely as $g = bh$ where $b \in B$ and $h \in H$. This decomposition is said to be a *gyrodecomposition* of the group G if

(i) H is a subgroup of G,
(ii)B is a subset of G such that $hBh^{-1} = B$ for all $h \in H$,
(iii) $1 \in B$, and
(iv) $B = B^{-1}$.

Let G be a group with a gyrodecomposition $G = BH$. The gyrodecomposition of $g_1 g_2 \in G$ gives the unique decomposition

$$g_1 g_2 = (g_1 \odot g_2) h(g_1, g_2)$$

where $g_1 \odot g_2 \in B$ and $h(g_1, g_2) \in H$. Foguel and Ungar [8] show that $(B, \odot)$ is a left gyrogroup with

$$gyr[g_1, g_2]g = h(g_1, g_2) g (h(g_1, g_2))^{-1}.$$

A subset K of a finite group G containing the identity 1 is a near subgroup if and only if for each $a, ax, ay \in K$, there is an element $af_a(x,y) = axyz \in K$, where z belongs to the commutator group of the group generated by $\{x, y\}$.

We ask the following question. When can the mappings f_a defining a near subgroup be chosen so that each operation $x \odot y = f_a(x,y)$ on $a^{-1}K$ is a left gyrogroup operation. If G has odd order, then every twisted subgroup K of G is a near subgroup of G. We can then indeed set $f_a(x,y) = x \oplus y = \sqrt{xy^2x}$, with gyrations given by $gyr[x,y] = \alpha(\sqrt{xy^2x}x^{-1}y^{-1})$, where $\alpha(h)$ is the inner automorphism of K given by $\alpha(h)k = hkh^{-1}$; this operation makes $(K, \oplus)$ a gyrocommutative gyrogroup, as shown by Foguel and Ungar [8].

Left gyrogroups satisfy a *left cancellation property*: For any $a, b \in K$, there is a unique element $x \in K$ such that $a = b \odot x$. A groupoid having an identity and satisfying the left cancellation property is called a *left loop*.

Theorem 8 *If each f_a defining a near subgroup K satisfies the left cancellation property (so that $a^{-1}K$ is a left loop), then the near subgroup K of G is a strong near subgroup of G.*

PROOF. Suppose K is not a strong near subgroup of G. Then some associate $L = a^{-1}K$ of K and some section $H^* = H/N$ are such that H^* is isomorphic to a dihedral group D_{2q} with q odd, and L^* consists of the involutions plus the identity in H^*. If bN is an involution in H^* with $b \in L \cap H$, then $b \odot x = f_a(b,x) = bxz$ must belong to $L \cap (N \cup bN)$ for all $x \in L \cap H$, so two such elements x, y will give $b \odot x = b \odot y$, contrary to uniqueness. □

We prove a converse. Gyrocommutative gyrogroups satisfy the *automorphic inverse property*: $x^{-1} \odot y^{-1} = (x \odot y)^{-1}$.

Theorem 9 *Suppose K is a strong near subgroup of G, and G is K-reduced. By Theorem 5, $G/O_2(G)$ is of odd order. We can define each f_a to satisfy the automorphic inverse property, and if $O_2(G)$ is abelian, to satisfy the left cancellation property as well, so that $a^{-1}K$ is a left loop.*

PROOF. We write each $x \in K$ as $x = ot$, where $o, t \in \langle x \rangle$ with o of odd order and t a 2-element. We define $f_1(ot, o't') = \sqrt{o}\sqrt{o'}tt'\sqrt{o'}\sqrt{o}$, which is in K because the 2-elements t, t' in K commute and K is a twisted subgroup. Note that f_1 satisfies the automorphic inverse property.

If $f_1(ot, o't') = f_1(ot, o''t'')$, then $\sqrt{o'}tt'\sqrt{o'} = \sqrt{o''}tt''\sqrt{o''}$. Writing $\sqrt{o''} = \sqrt{o'}t_1 = t_2\sqrt{o'}$ with $t_1, t_2 \in O_2(G)$, we have $tt' = t_1tt''t_2$. If $O_2(G)$ is abelian, then $t' = t_1t''t_2$, so $o't' = \sqrt{o'}t'\sqrt{o'} = \sqrt{o'}t_1t''t_2\sqrt{o'} = \sqrt{o''}t''\sqrt{o''} = o''t''$. □

Consider the 12-element group G with a normal subgroup N isomorphic to the elementary abelian group E_4 and G/N isomorphic to the cyclic group C_3, where if $N = \{1, a_1, a_2, a_3\}$, then some element $b \in G - N$ satisfies $b^3 = 1$ and $a_1b = ba_3$, $a_2b = ba_1$, $a_3b = ba_2$. Let K be the strong near subgroup $K = \{1, a_1, b, ba_2, b^2, b^2a_3\}$.

This is the smallest example of a strong near subgroup of a finite group where the conjugates of a 2-subgroup H_1 occurring in the characterization of K as a strong near subgroup are not all the same. Here $H_1 = \langle a_1 \rangle$, $H_b = \langle a_2 \rangle$, and $H_{b^2} = \langle a_3 \rangle$.

Left gyrogroups satisfy the *left inverse property (LIP)*: $x^{-1} \odot (x \odot y) = y$.

Proposition 1 *This example has exactly four operations $x \odot y = f_a(x,y) = xyz$ characterizing it as a near subgroup, for each $a \in K$, and satisfying the left cancellation property, so that $a^{-1}K$ is a left loop.*

(i) All four operations satisfy the LIP property.

(ii) Only two of these four operations make $a^{-1}K$ a left gyrogroup.

(iii) Only the other two of these four operations satisfy the automorphic inverse property (including the operation from Theorem 9).

(iv) None of the four operations makes $a^{-1}K$ a gyrogroup.

PROOF. The two operations f_1 are obtained by defining $K_i = \{1, a_i, b, ba_2, b^2, b^2a_3\}$, obtained from K by replacing a_1 with a_i. Thus $K_1 = K$, while K_2, K_3 are not twisted subgroups (so that some f_a cannot be defined for them). For $i = 2, 3$, each $x \in G$ has a unique decomposition $x = kh$ with $k \in K_i$ and $h \in \langle a_1 \rangle$. The left gyrogroup operation in K_i is given by the gyrodecompostion $xy = (x \odot y)h(x, y)$ with $gyr[x, y]k = h(x, y)kh(x, y)^{-1}$. The two operations in K are obtained with the correspondence that replaces a_i in K_i with a_1 in K. One can similarly obtain operations f_a for each $a \in K$ since each associate $L = a^{-1}K$ of K corresponds to K under an isomorphism of G.

We prove the claims stated in the proposition. Suppose $x \odot y = f_1(x, y) = xyz$ with z in the commutator group of the group $\langle x, y \rangle$. If x, y commute, then $x \odot y = xy$. Thus $x \odot 1 = 1 \odot x = x, b \odot b = b^2, b^2 \odot b^2 = b, b \odot b^2 = b^2 \odot b = 1, ba_2 \odot ba_2 = b^2a_3, b^2a_3 \odot b^2a^3 = ba_2, ba_2 \odot b^2a_3 = b^2a_3 \odot ba_2 = 1$.

Otherwise $x \odot y = xyz$ with z in the commutator of $\langle x, y \rangle$, which is contained in N. Combining this with the left cancellation property, where $x \neq y$ implies $z \odot x \neq z \odot y$, we get the following: $b \odot a_1 = ba_2, ba_2 \odot a_1 = b, b^2 \odot a_1 = b^2a_3, b^2a_3 \odot a_1 = b^2, b \odot ba_2 = b^2a_3, ba_2 \odot b = b^2, b^2 \odot b^2a_3 = ba_2, b^2a_3 \odot b^2 = b, b \odot b^2a_3 = a_1, b^2a_3 \odot b = a_1, b^2 \odot ba_2 = a_1, ba_2 \odot b^2 = a_1$.

Finally, either (1) $a_1 \odot b = b$ and $a_1 \odot ba_2 = ba_2$, or (2) $a_1 \odot b = ba_2$ and $a_1 \odot ba_2 = b$; either (3) $a_1 \odot b^2 = b^2$ and $a_1 \odot b^2a_3 = b^2a_3$, or (4) $a_1 \odot b^2 = b^2a_3$ and $a_1 \odot b^2a_3 = b^2$. There are thus four possible combinations.

Since $b \odot b^2a_3 = a_1$, the left gyroassociative law gives $b \odot (b^2a_3 \odot z) = a_1 \odot gyr[b, b^2a_3]z$. If (1) and (3) hold, then $gyr[b, b^2a_3]$ maps b to ba_2, and b^2 to b^2, contrary to gyroautomorphism. If (2) and (4) hold, then $gyr[b, b^2a_3]$ maps b tp b. and b^2 to b^2a_3, again contrary to gyroautomorphism.

The two remaining combinations, (1) and (4), or (2) and (3), give the two operations for $i = 2, 3$ defined above, and define left gyrogroups by the corresponding gyrodecomposition on K_i. These two operations do not satisfy the left loop property because $gyr[b, b^2a_3] \neq gyr[a_1, b^2a_3]$, and therefore do not define a gyrogroup. The operation f_1 from Theorem 9 gives (2) and (4) and is thus not a left gyrogroup.

Finally, for the combinations (1) and (3), or (2) and (4), the automorphic inverse property holds, while in the other two combinations (1) and (4), or (2) and (3), it does not since $a_1 \odot b^2 \neq (a_1 \odot b)^{-1}$. □

We generalize the phenomenon observed in the cases of Proposition 1 that give a left gyrogroup.

Theorem 10 *Let K be a strong near subgroup of G where G is K-reduced with corresponding automorphism $\tau = \tau_K$, so that $G/O_2(G)$ is of odd order. Assume*

(a) Every element of K is either a 2-element x or an element of odd order y;

(b) If $C(\tau)$ is the elements of G invariant under τ, then for some $t \in K$ with $t \neq 1$ and t of odd order, then $C(\tau)$ acts on H_{t^2} by conjugation; and

(c) If $x, y \neq 1$, where x is a 2-element in K and y is an element of odd order in K, then t from (b) acts on the commutator group of $\langle x, y \rangle$ by conjugation.

Then we can define the mapping $f_1(x, y) = xyz$ on K with z in the commutator of $\langle x, y \rangle$ to be a left gyrogroup operation $x \odot_1 y$ on K. This is derived from a gyrodecomposition $G = ((K - H_1) \cup H_{t^2})C(\tau)$ obtained from assumptions (a) and (b) alone.

PROOF. If $x \in H_1$, then $txt \in t^2H_{t^2}$, so $t^{-1}xt \in H_{t^2}$. Define $K_t = (K - H_1) \cup H_{t^2}$ obtained by replacing each element $x \in H_1$ with the corresponding element $t^{-1}xt \in H_{t^2}$.

We obtain a gyrodecomposition $G = K_tH$ with $H = C(\tau)$. Define $g(z) = z(\tau(z))^{-1}$ If $g(z)$ is not in $O_2(G)$, then

$$z = (\sqrt{g(z)})(\sqrt{g(z)}\tau(z))$$

decomposes z as $z = bh$ with $b \in K_t$ and $h \in C(\tau)$. Indeed, if $z = a_1a_2\cdots a_n$ with each $a_i \in K$, then $g(z) = a_1a_2\cdots a_na_n\cdots a_2a_1 \in K$ because K is a twisted subgroup of G, and so $g(z) \in K - H_1$. Furthermore if $h = \sqrt{g(z)}\tau(z)$, then $h = \tau(h)$ because $h(\tau(h))^{-1} = \sqrt{z(\tau(z))^{-1}}\tau(z)z^{-1}\sqrt{z(\tau(z))^{-1}} = 1$.

If $g(z)$ is in $O_2(G)$, then

$$z = t^{-2}(t^2z) = (t^{-2}\sqrt{g(t^2z)})(\sqrt{g(t^2z)}\tau(t^2z))$$

again decomposes z as $z = bh$ with $b \in K_t$ and $h \in C(\tau)$. Indeed $g(t^2z) \in t^4H_{t^4}$, so $\sqrt{g(t^2z)} \in t^2H_{t^2}$ and $t^{-2}\sqrt{g(t^2z)} \in H_{t^2}$, while $\tau(h) = h$ as before.

We show that this decomposition is unique. Suppose to the contrary that $y, z \in K_t$ with $y \neq z$ and $z = yx$ with $x \in H$. Suppose first $y, z \in K - H_1$, so that y, z are of odd order. $(yx)^{-1} = \tau(yx) = y^{-1}x$, so $y^{-1}xy = x^{-1}$. Then $y^{-2}xy^2 = x$, so y^2 and x commute, and therefore y and x commute so that $y^{-1}xy = x$, thus $x = x^{-1}$ and so $x^2 = 1$. This implies that if y is of odd order, then $|z| = |yx| = 2|y|$, contrary to the assumption that z is also of odd order.

If $y, z \in H_{t_2}$, then $t^2y, t^2z \in t^2H_{t^2} \subseteq K - H_1$, and we are back to the previous case. If $y \in H_{t_2}$ and $z \in K - H_1$, then we consider the odd order group $G^* = G/O_2(G)$. Then $y^*, z^* \in K^*$ and $x^* \in C(\tau^*)$, but $y^* = 1$, so $z^* = x^*$ with $\tau^*(x^*) = x^*$ and $\tau(z^*) = (z^*)^{-1}$, which is not possible since $z^* \neq 1$ is of odd order.

The gyrodecomposition axioms for the unique decomposition $G = K_tH$ are verified since $1 \in K_t$ and $K_t^{-1} = K_t$, $hKh^{-1} = K$ for all $h \in C(\tau)$ because K is a twisted subgroup of G, so that $h(K - H_1)h^{-1} = (K - H_1)$, and $hH_{t^2}h^{-1} = H_{t^2}$ by assumption (b), so $hK_th^{-1} = K_t$.

We thus obtain a left gyrogroup $(K_t, \odot)$ from assumptions (a) and (b) alone, with the decomposition $xy = (x \odot y)h(x, y)$ with $gyr[x, y]k = h(x, y)kh(x, y)^{-1}$.

Back in K, using the correspondence of $x \in H_1$ with $t^{-1}xt \in H_{t^2}$, we obtain a left gyrogroup $(K, \odot_1)$ given by:

(1) $x \odot_1 y = x \odot y = \sqrt{g(xy)} = \sqrt{xy^2x}$ if $x, y, xy \notin O_2(G)$;
(2) $x \odot_1 y = t(t^{-1}xt \odot t^{-1}yt)t^{-1} = xy$ if $x, y \in O_2(G)$;
(3) $x \odot_1 y = t^{-1}xt \odot y = \sqrt{g(t^{-1}xty)} = \sqrt{t^{-1}xty^2txt^{-1}}$ if $x \in O_2(G), y \notin O_2(G)$;
(4) $x \odot_1 y = x \odot t^{-1}yt = \sqrt{g(xt^{-1}yt)} = \sqrt{xt^{-1}yt^2yt^{-1}x}$ if $x \notin O_2(G), y \in O_2(G)$;
(5) $x \odot_1 y = t(x \odot y)t^{-1} = t(t^{-2}\sqrt{g(t^2xy)})t^{-1} = t^{-1}\sqrt{t^2xy^2xt^2}t^{-1}$ if $x, y \notin O_2(G), xy \in O_2(G)$.

We verify that $x \odot_1 y = xyz$ with z in the commutator R of $V = \langle x, y\rangle$. This is clear in cases (1) and (2). For the remaining cases, consider the abelian group $V^* = V/R$. We have $K^* = V^*$. We must have $V = \langle y\rangle R$ in case (3) and $V = \langle x\rangle R$ in cases (4),(5), because otherwise V contains an element of K that is neither a 2-element nor of odd order, contrary to condition (a). We also have $t^{-1}Rt = R$ in cases (3),(4) by condition (c), and also in case (5) because $y = (\sqrt{x})^{-1}u(\sqrt{x})^{-1}$ with $u \in H_1$, so $\langle x, y\rangle = \langle x, u\rangle$. It then follows that $x \odot_1 y \in yR$ in case (3), $x \odot_1 y \in xR$ in case (4), and $x \odot y \in R$ in case (5), thus verifying that $x \odot_1 y = xyz$ with $z \in R$ in these three cases as well. $\square$

Aschbacher [4] starts with an assumption essentially equivalent to (a) and obtains a left gyrogroup operation that may or may not satisfy $f_1(x,y) = xyz$ with z in the commutator of $\langle x, y\rangle$. Let K be a strong near subgroup of G such that G is K-reduced. Let $Q = O_2(G)$, and let $H = C_G(\tau)$ be the elements of G that are invariant under τ. Aschbacher assumes

(*) For each $1 \neq k \in K$ of odd order, $C_Q(k) = 1$.

Here $C_Q(k) = \{x \in Q : kx = xk\}$. Under this sole assumption, he shows:

(1) Q is abelian.
(2) $|Q| = |H_1|^2$ and $|H_1| = |C_Q(\tau)|$
(3) There is an X-invariant complement Q_0 to $C_Q(\tau)$ in Q, where X is a Hall $2'$-subgroup of $C_G(\tau)$
(4) Let $K_0 = \{k \in K : 1 \neq |k| \text{ is odd}\}$, and let $J = K_0 \cup Q_0$. Then $G = JH$ is a gyrodecomposition of G, so J is a left gyrogroup with operation $\odot$.
(5) $\pi : Q_0 \to H_1$ defined by $\pi(u) = g(u) = u(\tau(u))^{-1}$ is an X-isomorphism of Q_0 wit H_1.
(6) $K = K_0 \cup H_1$.
(7) Extend π to $\pi : J \to K$ by defining $\pi(k) = k$ for each $k \in K_0$ and define the operation $*$ on K by $a * b = \pi(\pi^{-1}(a) \odot \pi^{-1}(b))$. Then $K, *$ is a left gyrogroup such that $b^{-1}a^{-1}(a * b)$ is in the commutator group of $\langle a, b\rangle$ for $a, b \in K$, except possibly if $a \in H_1$ and $b \in K_0$.

Indeed, if we write $x = \pi(i)$ and $y = \pi(j)$ for $x, y \in H_1$, then

(1) $x * y = x \odot y = \sqrt{g(xy)} = \sqrt{xy^2x}$ if $x, y, xy \notin O_2(G)$;
(2) $x * y = g(i \odot j) = g(ij) = xy$ if $x, y \in O_2(G)$;
(3) $x * y = g(x \odot y) = g(xy) = xy^2x$ if $x, y \notin O_2(G), xy \in O_2(G)$;
(4) $x * y = x \odot j = \sqrt{g(xj)} = \sqrt{xyx}$ if $x \notin O_2(G), y \in O_2(G)$;
(5) $x * y = i \odot y = \sqrt{g(iy)} = \sqrt{iy^2i^{-1}x}$ if $x \in O_2(G), y \notin O_2(G)$.

Thus $x * y = xyz$ with z in the commutator group of $\langle x, y\rangle$ except possibly in case (5). It is possible to achieve this property in case (5) by a choice of a specific Q_0 in some cases. Indeed, Aschbacher has indicated that this property is achieved both here and with the construction of Theorem 10 if G/Q is a p-group, but this is not possible if G/Q is the direct product C_pC_q of two cyclic groups of different prime orders p, q.

Say that G is *strongly K-reduced* if whenever N is a normal subgroup of G such that $aN \subseteq K$ for all $a \in K$, then $N = 1$. One can always find such an N so that $G^* = G/N$ is strongly K^*-reduced. If K is a strong near subgroup of G, where G is K-reduced, and we select such an N so that $G^* = G/N$ is strongly K^*-reduced, then $N \cap O_2(G)$ is the intersection of the H_a.

Aschbacher [4] remarks that if G is strongly K-reduced for a strong near subgroup K, and G/Q is cyclic of odd order for $Q = O_2(G)$, then Q is abelian. This allows us to remove the assumption that Q is abelian from Theorem 9.

Theorem 11 *Suppose K is a strong near subgroup of G, and G is K-reduced. By Theorem 5, $G/O_2(G)$ is of odd order. We can define each $f_a(x,y) = xyz$ on $a^{-1}K$ with z in the commutator of $\langle x,y\rangle$ to be a left loop satisfying both the automorphic inverse property and the left cancellation property.*

Proof. Again write each $x \in K$ as $x = ot$, where $o, t \in \langle x\rangle$ with o of odd order and t a 2-element, and define $f_1(ot, o't') = \sqrt{o}\sqrt{o'}tt'\sqrt{o'}\sqrt{o}$ satisfying the automorphic inverse property.

If $f_1(ot, o't') = f_1(ot, o''t'')$, then $\sqrt{o'}tt'\sqrt{o'} = \sqrt{o''}tt''\sqrt{o''}$. Let $Q = O_2(G)$, $G' = \langle o'\rangle Q = \langle o''\rangle Q$, $K' = K \cap G'$, $G'' = \langle K'\rangle$, and $Q' = Q \cap G''$. By Aschbacher's remark, Q' contains a normal subgroup N of G'' such that $aN \subseteq K'$ for all $a \in K'$, and $Q^* = Q'/N$ is abelian.

Applying Theorem 9 in $G^* = G''/N$, we conclude that $\sqrt{o'}^* = \sqrt{o''}^*$, so $\sqrt{o''} = \sqrt{o'}u = v\sqrt{o'}$ with $u, v \in N$. We have $tt' = utt''v$, so $t' = ut''v$, and so $o't' = \sqrt{o'}t'\sqrt{o'} = \sqrt{o'}ut''v\sqrt{o'} = \sqrt{o''}t''\sqrt{o''} = o''t''$. $\square$

Note that we can not in general simultaneously require that the left loop $x \odot_a y = xyz$ with z in the commutator group of $\langle x,y\rangle$ be a left gyrogroup operation and satisfy the automorphic inverse property as in Theorem 11, as shown by the example of Proposition 1.

Aschbacher [4] has also shown that if G is strongly K-reduced for a strong near subgroup K, and G/Q is abelian of odd order for $Q = O_2(G)$, then Q is abelian. He then obtains a gyrodecomposition $G = JH$ with $H = C_G(\tau)$ and thus a left gyrogroup J related to K. A correspondence between J and K gives a left gyrogroup operation $*$ on K, where $b^{-1}a^{-1}(a*b)$ is in the commutator group of $\langle a,b\rangle$, provided either a is of odd order or b is a 2-element.

Indeed, if we write $a = ot$ with $o, t \in \langle x\rangle$, o of odd order and t a 2-element, then $a = ot \in K$ corresponds to $oi \in J$ with $g(i) = t$. Then $ot * o't' = o''t''$ corresponds to $oi \odot o'i' = o''i''$, so

$$oio't'o'i^{-1}to = g(oio'i') = g(o''i'') = o''t''o''.$$

If $t = i = 1$ or $o' = 1$, then i and o' commute, so $oo't'o'to = o''t''o''$, and therefore $o''t'' \in \langle ot, o't'\rangle$ with $\overline{o''} = \overline{o}\overline{o'}$ and $\overline{t''} = \overline{t}\overline{t'}$.

Acknowledgements

The author had very valuable conversations with Michael Aschbacher, Tuval Foguel, Michael Kinyon, and Abraham Ungar.

References

[1] M. Aschbacher. "Finite group theory". Cambridge University Press (1986).

[2] M. Aschbacher. "Near subgroups of finite groups". Journal of Group Theory 1 (1998) 113–119.

[3] M. Aschbacher. Manuscript 1 (2001).

[4] M. Aschbacher. Manuscript 2 (2001).

[5] R. Baer. "Nets and groups I". Trans. Amer. Math. Soc. 46 (1939) 110-141.

[6] T. Feder and M. Vardi. "The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory". SIAM Journal on Computing 28 (1998) 57–104.

[7] T. Feder. "Constraint satisfaction on finite groups with near subgroups". Submitted to SIAM Journal on Computing (2001).

[8] T. Foguel and A.A. Ungar. "Involutory decomposition of groups into twisted subgroups and subgroups". J. Group Theory 3 (2000) 27–46.

[9] G. Glauberman. "On loops of odd order ". Journal of Algebra 1 (1964) 374–396.

[10] G. Glauberman. "On loops of odd order II". Journal of Algebra 8 (1968) 393–414.

[11] M. Kikkawa. "The geometry of homogeneous Lie loops" Hiroshima Math. J. 5 (1975) 141-179.

[12] M. Kikkawa. "On some quasigroups of algebraic models of symmetric spaces". Mem. Fac. Lit. Sci. Shimane Univ. (Nat. Sci.) 6 (1973) 9-13.

[13] A. Kreuzer. "Inner mappings of Bruck loops". Math. Proc. Cambr. Phil. Soc. 123 (1998) 53-57.

[14] J.D. Phillips. "Right quotients of groups". Comm. Alg. 25 (1997) 1341-1345.

[15] L.V. Sabinin. "On the equivalence of categories of loops and homogeneous spaces". Soviet Math. Dokl. 13 (1972) 970-974.

[16] A.A. Ungar. "Thomas precession: its underlying gyrogroup axioms and their use in hyperbolic geometry and relativistic physics". Found. Phys. 27 (1997) 881–951.

[17] A.A. Ungar. "Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession: The Theory of Gyrogroups and Gyrovector Spaces". Dordrecht, Boston, London: Kluwer Acad. Publ. (2001).