Near-factors of finite groups

D. de Caen, D.A. Gregory, I.G. Hughes

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, Canada
K7L 3N6

D.L. Kreher

School of Computer Science
Rochester Institute of Technology
Rochester, N.Y. 14623

Abstract. Let S and T be subsets of a finite group G with identity e. We write $G-e = ST$ if every non-identity element g can be written uniquely as $g = st$ with $s \in S$ and $t \in T$. These near-factorizations are motivated by the combinatorial problem of finding $(0,1)$-matrix factorizations of the matrix $J-I$. We derive some results on near-factors S and T. For example, S and T each generate G. Also, if G is abelian, then the automorphism $g \rightarrow g^{-1}$ is a multiplier of both S and T. If the elementary abelian group C_p^n (p an odd prime) is a homomorphic image of G, then $|S|^{p-1} \equiv |T|^{p-1} \equiv 1 \pmod{p^n}$. These structure theorems suggest that noncyclic abelian groups rarely have near-factorizations. Constructions of near-factorizations are given for cyclic groups and dihedral groups.

1. Introduction

This paper is motivated by the study of $(0,1)$-factorizations of the matrix $J-I$. Here J is the $n \times n$ all ones matrix and I is the $n \times n$ identity matrix. We first recall a theorem concerning such factorizations.

Theorem 1. ([1; thm. 1.2], see also [2; thm. 3.4]) *Let r, s be integers and suppose that $rI + sJ = AB$ where A and B are $n \times n$ nonnegative integral matrices. If r and s are relatively prime, then A and B have contant line sums; that is, there are integers, a and b say, such that each row and column sum of A is a, and each row and column sum of B is b. Furthermore, $AB = BA$.*

Let $J - I = AB = XY$ be two $(0,1)$-factorizations of $J - I$. We say that these factorizations are *equivalent* if there exist $n \times n$ permutation matrices P and Q such that either either $X = PAQ$ and $Y = Q^tBP^t$, or $Y^t = PAQ$ and $X^t = Q^tBP^t$. It is natural to seek a classification of the inequivalent $(0,1)$-factorizations of $J-I$. However, this is probably too difficult. For example, Lam [4] and others have studied special cases where Y is a power of X; that is, they examine the equation $X^k = J-I$. Some constructions are known, but a complete classification is nowhere in sight at present. Here we will examine another special case, the factorizations into group matrices.

Definition: Let G be a finite group of order n with identity e. A *near-factorization* of G is a pair of subsets S and T of G such that each $g \in G, g \neq e$, can be written uniquely as $g = st$ for some $s \in S$ and $t \in T$. We assume that e cannot be written as a product st. Also, to exclude trivial factorizations, we assume that $1 < |S| < n-1$ always.

We denote a near-factorization by $G - e = ST$. The sets S an T will be called *near-factors* of G.

If the elements of G are taken in some order G_i, $i = 1, 2, \ldots, n$, then to each subset R of G we can associate an $n \times n$ $(0,1)$-matrix $M(R)$ with i, j^{th} entry equal to 1 if $g_i^{-1} g_j \in R$, and 0 otherwise. We call $M(R)$ a group matrix. It is easily seen that

$$ST = G - e$$

is a near-factorization of G if and only if

$$M(S)\,M(T) = M(G \backslash e) = J - I$$

Example 1: If C_n is the cyclic group of order n and g is any generator, then

$$C_n - e = \{g, g^2, g^3, \ldots, g^s\}\{e, g^s, g^{2s}, \ldots, g^{(t-1)s}\} \tag{1}$$

whenever $n - 1 = st$. If t in turn has a factorization $t = uv$ and we let $h = g^s$, then the second near-factor in (1) can be factored further:

$$\{e, h, h^2, \ldots, h^{t-1}\} = \{e, h, h^2, \ldots, h^{u-1}\}\{e, h^u, h^{2u}, \ldots, h^{(v-1)u}\}.$$

Continuing in this manner, we see that if g is any generator of C_n, and $n - 1 = n_1 n_2 \ldots n_k$ is any factorization of $n - 1$, then

$$C_n - e = g \prod_{i=1}^{k} \{e, g_i, g_i^2, \ldots, g_i^{(n_i - 1)}\}$$

where $g_1 = g$ and $g_{i+1} = (g_i)^{n_i}$ for $i = 1, 2, \ldots, k-1$. In particular, if $n = m^k + 1$, then,

$$C_n - e = g \prod_{i=0}^{k-1} \{e, g^{m^i}, g^{2m^i}, \ldots, g^{(m-1)m^i}\}.$$

Also, if $n = k! + 1$, then

$$C_n - e = g \prod_{i=1}^{k-1} \{e, g^{i!}, g^{2i!}, \ldots, g^{i \cdot i!}\}.$$

These sets can be multiplied together in various ways to give near-factorizations of C_n that are not equivalent to (1).

Example 2: Let D_n be the dihedral group of order $2n$, with presentation $D_n = \{x, y | x^2 = y^n = e, xy = y^{-1}x\}$. If k is a divisor of $2n-1$, then we have the near-factorization $D_n - e = ST$, where

$$S = \{y^i : 1 \leq i \leq (k-1)/2\} \cup \{xy^i : 0 \leq i \leq (k-1)/2\}, \text{ and,}$$
$$T = \{y^{jk} : 0 \leq jk < n\} \cup \{xy^{jk} : 0 < jk < n\}$$

The verification that this gives a near-factorization of D_n is straightforward.

The remainder of the paper is devoted to structural and non-existence theorems. Throughout, G will be a multiplicative group of order n with identity element e. If $G - e = ST$ is a near-factorization of G, then clearly $(n-1) = |S||T|$ where the vertical bars denote the cardinality of a set. Thus if $(n-1)$ is prime then G has no near-factorizations. Let $\langle S \rangle$ denote the subgroup of G generated by S.

Proposition 1. *If $G - e = ST$ is a near-factorization of G, then*

$$\langle S \rangle = \langle T \rangle = G$$

Proof: Let $H = \langle S \rangle \neq \{e\}$ and suppose that $H \neq G$. Let $G = H \cup Hg_1 \cup \ldots \cup Hg_k$ be a right coset decomposition. As $S \subseteq H$, each translate $St, t \in T$ is contained entirely in some right coset. Thus Hg_1 is partitioned into certain right translates of S. Therefore $|S|$ divides $|H|$, which in turn divides n by Lagrange's theorem. However, $|S|$ also divides $n-1$ and so $|S| = 1$, a contradiction. ▮

Example 3: Suppose G has order 27. Since $27 - 1 = 2 \times 13$, any near-factorization of G would have say, $|S| = 2$ and $|T| = 13$. So let $G - e = \{x, y\}T$. Then $\{e, yx^{-1}\} \cdot xT$ is also a near-factorization and so, by proposition 1, $G = \langle e, yx^{-1} \rangle$. Thus $G = \langle yx^{-1} \rangle$ is necessarily cyclic.

2. Symmetry of near-factors in abelian groups

A *generalized permutation matrix* has all entries ±1 or 0, and precisely one non-zero entry in each row and column.

Theorem 2. *Let k be an integer and let $kJ - I = XY$ be a factorization into $n \times n$ integral matrices X and Y having constant line sums r and s, respectively. Suppose that X is normal; that is, $XX^t = X^tX$. Then there is a generalized permutation matrix P such that $X^t = PX$.*

Proof: It is easy to see that $kJ - I$ is invertible with inverse $-I + \frac{k}{nk-1}J$. From $kJ - I = XY$ we have

$$X^{-1} = Y(kJ - I)^{-1} = -Y + \frac{sk}{nk-1}J$$

and thus

$$X^tX^{-1} = -X^tY + \frac{rsk}{nk-1}J = -X^tY + kJ.$$

In particular, the matrix $M = X^tX^{-1}$ has integer entries. Furthermore, as X is normal,

$$MM^t = X^tX^{-1}(X^{-1})^tX = X^t(X^t)^{-1}X^{-1}X = I.$$

It follows easily that M is a generalized permutation matrix. ▮

Definition: Given a subset S of a group G, let $\overline{S} = \{h^{-1} : h \in S\}$. Then S is called *shift-symmetric* if $\overline{S} = gS$ for some $g \in G$.

Corollary 1. *Let $G - e = ST$ be a near-factorization of the abelian group G. Then S and T are shift-symmetric.*

Proof: Note that $M(\overline{S}) = M(S)^t$. Since G is abelian, $M(S)$ is normal and so Theorem 2 applies to give $M(\overline{S}) = PM(S)$ for some generalized permutation matrix P. Since $M(\overline{S})$ and $M(S)$ are $(0,1)$-matrices, then P is in fact a permutation matrix. Also $P = M(g)$ for some $g \in G$ since these are the only group matrices over G that are permutation matrices. Hence $M(\overline{S}) = M(gS)$ and so $\overline{S} = gS$. ▮

The statement that S is shift-symmetric is equivalent (in design theoretic parlance [5]) to the statement that the automorphism $g \to g^{-1}$ is a multiplier of the near-factor S, provided that G is abelian. It would be interesting to find other such multiplier theorems.

Corollary 1 is a useful tool in the study of near-factorizations of abelian groups. We first show that the near-factors S and T may be assumed to be symmetric.

Proposition 2. *If an abelian group G has a near-factorization $G - e = ST$, then it has a near-factorization $G - e = UV$ with $|U| = |S|$ and $|V| = |T|$, $\overline{U} = U$ and $\overline{V} = V$.*

Proof: We have $\overline{S} = gS$ for some $g \in G$, by Corollary 1. We shall prove that $g = x^2$ for some $x \in G$; we may then take $U = xS$, $V = x^{-1}T$. To show that g is a square, first note that if G is of odd order $2k + 1$, then $g^{2k+1} = 1$ and so $g = (g^{-k})^2$. If G is of even order, then S and T each have an odd number of elements since $|S||T| = |G| - 1$. Consider the mapping $F(h) = g^{-1}h^{-1}$. If $h \in S$, then $g^{-1}h^{-1} \in g^{-1}\overline{S} = g^{-1}gS = S$. Thus we may view F as a permutation of the set S. Since F is an involution and $|S|$ is odd, F has a fixed point $y \in S$. Thus $y = F(y) = g^{-1}y^{-1}$ and so $g = y^{-2}$ is a square. ▮

Proposition 3. *Let G be an abelian group and $G - e = ST$ a near-factorization with $|S| \leq 4$. Then G must be a cyclic group.*

Proof: We have $|S| = 2, 3$, or 4. If $|S| = 2$, then the argument of Example 3 given earlier applies (the assumption that G is abelian is not even needed in this case). If $|S| = 3$, then by Proposition 2 we may assume that $\overline{S} = S$, so either $S = \{x, x^{-1}, y\}$ where $y = y^{-1}$ or $S = \{x, y, z\}$ where $x^2 = y^2 = z^2 = 1$. In the latter case, we see by Proposition 1 that G is C_2^2 or C_2^3, both of which are easily discounted. In the first case, $G - e = \{yx, y^{-1}x^{-1}, e\} \cdot yT$ and so by Proposition 1, $G = \langle xy \rangle$.

If $|S| = 4$ and $S = \overline{S}$, then necessarily $S = \{x, x^{-1}, y, y^{-1}\}$ for some x and y (note that G has odd order and so has no elements of order 2). But $\{x, x^{-1}, y, y^{-1}\} = \{e, xy\} \cdot \{x^{-1}, y^{-1}\}$. Thus $\{e, xy\}$ is a near-factor of G and so $G = \langle xy \rangle$ by Proposition 1. ∎

Example 4: By Proposition 3, the group C_5^2 has no near-factorization.

Let $C_p - e = ST$ be a near-factorization of the cyclic group C_p, p an odd prime. If ω is a complex p^{th} root of unity, then the near factorization yields the equation

$$-1 = \left(\sum_{i \in S} \omega^i\right)\left(\sum_{j \in T} \omega^j\right).$$

Thus the complex number $u = \sum_{i \in S} \omega^i$ is a unit in $\mathcal{Z}[\omega]$, the ring of algebraic integers in the cyclotomic field $\mathbf{Q}(\omega)$. A theorem of Kummer [6, p. 10] asserts that if u is any unit in $\mathcal{Z}[\omega]$, then $\overline{u} = \omega^k u$ for some k, where $\overline{u}$ is the complex conjugate of u. It is this result that originally led us to conjecture Corollary 1. Conversely, one can give a new proof of Kummer's theorem using the method of Theorem 2; we now outline such a proof:

Let $u = \sum_{i=0}^{p-1} a_i \omega^i$ be a unit in $\mathcal{Z}[\omega]$ and let $v = \sum_{i=0}^{p-1} b_i \omega^i$ be a unit with $uv = 1$. For x a generator of C_p, define $\widehat{u}$ by $\widehat{u} = \sum_{i=0}^{p-1} a_i x^i$ and $\widehat{v}$ similarly; u and v are members of the group ring $\mathcal{Z}C_p$. It is not difficult to show that $\widehat{u}\widehat{v} = lC_p + e$ for some integer l (for this use the fact that $1 + t + \ldots + t^{p-1}$ is the minimal polynomial of ω). Because of a natural correspondence between group matrices and members of the group ring, it follows from Theorem 2 that $\widehat{u}$ is a shift-symmetric element of $\mathcal{Z}C_p$, that is,

$$\sum_{i=0}^{p-1} a_i x^{-i} = x^k \sum_{i=0}^{p-1} a_i x^i$$

for some k. Putting $x = \omega$ gives the desired conclusion.

3. A congruential criterion

We refer to Sehgal [8] for the terminology and basic concepts of group rings. Identifying S, T, G with $\sum_{s \in S} s$, $\sum_{t \in T} t$, $\sum_{g \in G} g$, respectively, we see that a near factorization $ST = G - e$ can be regarded as an equation in the group ring $\mathcal{Z}G$ of G over the integers $\mathcal{Z}$.

If $\sigma : G \rightarrow H$ is a homomorphism of G onto a group H, then we may extend σ to a group ring homomorphism $\sigma : \mathcal{Z}G \rightarrow \mathcal{Z}H$ by taking $\sigma(A) = \sum_g a_g \sigma(g)$

for each $A = \sum_g a_g g$ in $\mathbb{Z}G$. In particular, if $\iota : G \to \{1\}$ is the constant homomorphism $\iota(g) = 1 \in \mathbb{Z}$ for all $g \in G$, then the extension of ι to $\mathbb{Z}G$ is the augmentation map: $\iota(A) = \sum_g a_g$, for each $A \in \mathbb{Z}G$. We write $|A|$ for $\iota(A)$. We use $\bar{\ }$ to denote the extension of the inversion automorphism: $\overline{A} = \sum_g a_g g^{-1}$.

Theorem 3. *If the (not necessarily abelian) group G has the elementary abelian group C_p^m as a quotient group, then for any near-factorization $G - e = ST$,*

$$|S|^{p-1} \equiv |T|^{p-1} \equiv 1 \pmod{p^m} \text{ if } p \text{ is an odd prime, while}$$
$$|S| \equiv -|T| \equiv \pm 1 \pmod{2^m} \text{ if } p = 2$$

Proof: Let $q = p^m$ and let $\widehat{\ } : G \to H$ be a homomorphism of G onto $H = C_p^m$. Regarding S and T as members of the group ring $\mathbb{Z}G$ and extending $\widehat{\ }$ to a group ring homomorphism $\widehat{\ } : \mathbb{Z}G \to \mathbb{Z}H$, we have $AB = kH - e$ where $A = \widehat{S}$, $B = \widehat{T}$ and $k = |G|/q$.

If σ is an automorphism of H, extend σ to an automorphism of $\mathbb{Z}H$ to obtain $\sigma(A)\sigma(B) = kH - e$. Let $N(A) = \prod_{i=1}^{q-1} \sigma^i(A)$ where σ is an automorphism of H of order $q - 1$. (Any generator of the multiplicative group of the field $GF(q)$ yields such a σ.) Defining $N(B)$ analogously, we obtain

$$N(A)N(B) = (kH - e)^{q-1} = rH \pm e \tag{2}$$

for some integer r. The members $N(A)$, $N(B)$ of $\mathbb{Z}H$ are invariant under σ. Since σ is transitive on $H - e$, it follows that $N(A) = ae + bH$ and $N(B) = ce + dH$ for some integers a, b, c, d. Substitution in (2) gives $ac = \pm 1$, so $a^2 = c^2 = 1$. Applying the augmentation map to $N(A)$ gives

$$|S|^{q-1} = |A|^{q-1} = |N(A)| = a + bq, \text{ so } |S|^{2(q-1)} \equiv 1 \pmod{q}.$$

The number of integers less than and relatively prime to q is $\varphi = p^{m-1}(p-1)$. Since $|S|$ and q are relatively prime, we also have $|S|^{\varphi} \equiv 1 \pmod{q}$. As the greatest common divisor of $2(q-1)$ and φ is $p - 1$ if p is odd and 2 if $p = 2$, we finally obtain $|S|^{p-1} \equiv 1 \pmod{q}$ if p is an odd prime and $|S|^2 \equiv 1 \pmod{2^m}$ if $p = 2$. Similar congruences hold for $|T|$. Since $|S||T| = |G| - 1 \equiv -1 \pmod{q}$, the congruences stated in the theorem are true. ∎

Example 5: Let p be an odd prime. Since $p^2 - 1 = (p-1)(p+1)$, one may look for a near-factorization $C_p \times C_p - e = ST$ with $|S| = p - 1$, and $|T| = p + 1$. However, by the binomial theorem,

$$|S|^{p-1} = (p-1)^{p-1} \equiv -p + 1 \not\equiv 1 \pmod{p^2}.$$

Hence by Theorem 3 such a near-factorization does not exist.

The congruence $|S|^{p-1} \equiv 1 \pmod{p^2}$ is of interest in its own right because of its connection with Fermat's Last Theorem [3]. A machine search reveals that only 19 of the 1163 prime p less than 10,000 are such that $p^2 - 1 = st$, $s, t > 4$, and $s^{p-1} \equiv 1 \pmod{p^2}$. In particular C_p^2, p a prime less than 29, has no near-factorization.

The non-cyclic elementary abelian group of smallest order that satisfies the congruence in Theorem 3 for some $|S|, |T| \geq 4$ is C_7^3. Here $7^3 - 1 = 18 \times 19$ where $18^6 \equiv 1 \pmod{7^3}$. We do not know if C_7^3 has a near-factorization.

4. Further non-existence theorems, with emphasis on abelian groups of small order

Proposition 4. *Suppose that $G - e = ST$ is a near-factorization of G and that $\hat{}\, : G \to H$ is a homomorphism of G onto a group H. For each $h \in H$ let $s(h) = \{g \in S : \hat{g} = h\}$ and $t(h) = \{g \in t : \hat{g} = h\}$. Then*

(i) $\sum |s(h)| = |S|, \sum |t(h)| = |T|$

(ii) $\sum |s(h)||t(h^{-1})| = |G|/|H| - 1$

(iii) $\sum |s(h)||t(h^{-1}k)| = |G|/|H|$ *for all* $k \in H, k \neq e$

where each of the summation is taken over all $h \in H$. Moreover, if $\overline{S} = S$, $\overline{T} = T$, then

(iv) $s(h^{-1}) = \overline{s(h)}$ *and* $t(h^{-1}) = \overline{t(h)}$ *for all* $h \in H$.

Proof: Equations (i), (ii), (iii) are restatements of the equalities $|\widehat{S}| = |S|$, $|\widehat{T}| = |T|$, and $\widehat{S}\widehat{T} = rH - e$, where $r = |G|/|H|$. ∎

Example 6: We will show that $G = C_5 \times C_5 \times C_2$ has no near-factorization. Suppose then that $G - e = ST$ where, necessarily, $|S| = |T| = 7$. By Proposition 2, we may assume that S and T are symmetric: $\overline{S} = S$ and $\overline{T} = T$. We regard G as an additive group, taking its elements to be all triples (x, y, z) of integers $0 \leq x, y \leq 4, 0 \leq z \leq 1$. Since S and T have odd cardinality and are closed under inversion, each must contain an odd number (and hence one) of the elements of order 1 or 2: $(0,0,0), (0,0,1)$. Since $S + (0,0,0), T + (0,0,1)$ are also symmetric near-factors, we may assume that $(0,0,0) \in S$ and so $(0,0,1) \in T$. If f is an invertible linear map on the vector space $C_5 \times C_5$ then the map F on G defined by $F(x, y, z) = (f(x, y), z)$ is an automorphism. Since $\langle S \rangle$ generates G (Proposition 1), by using such a linear map if necessary, we may assume that $(1, 0, a)$ and $(0, 1, b)$ are in S for some integers $0 \leq a, b \leq 1$. Thus we may take

$$S = \{(0,0,0), \pm(1,0,a), \pm(0,1,b), \pm(u,v,c)\}$$

where $0 \leq a, b, c \leq 1$. By using one of four linear maps $f(x, y) = (\pm x, \pm y)$ if necessary, we may also assume that $0 \leq u, v \leq 2$. Given this pattern for S, a little checking shows that for each of the two homomorphisms $\hat{}\, : G \to C_5$ given by

$\widehat{(x,y)} = x$ or y, the only feasible distributions for the equations in Proposition 4 are:

$$(|s(0)|,|s(1)|,|s(2)|,|s(3)|,|s(4)|) = (3,2,0,0,2),$$
$$(|t(0)|,|t(1)|,|t(2)|,|t(3)|,|t(4)|) = (3,0,2,2,0).$$

Thus, $u = v = 1$. Note that the homomorphism $(x,y,z) \rightarrow x - y$ satisfies this distribution for S and therefore must also do so for T. A little thought now shows that

$$T = \{(0,0,1), \pm(2,0,x), \pm(0,2,y), \pm(2,2,z)\}$$

for some integers $0 \leq x,y,z, \leq 1$. Now $(2,2,z) = (0,0,0) + (2,2,z)$ and $(2,2,z{+}c) = -(1,1,c) - (2,2,z)$. Therefore, $c = 1$; otherwise $(2,2,z)$ could be written two different ways using elements of S and T. Likewise, $(-2,0,x) = (0,0,0) - (2,0,x)$, $(-2,0,a+x) = (1,0,a) + (2,0,x)$ imply that $a = 1$; and, $(1,0,a+1) = (1,0,a) + (0,0,1)$, $1,0,x+a) = (2,0,x) - (1,0,a)$ imply that $x = 0$. Similarly, $b = 1$ and $y = 0$. But then $(1,0,a) + (0,2,y) = -(1,0,a) + (2,2,z)$, a contradiction.

The next theorem uses a property of characters of abelian groups of exponent 2, 3, 4 or 6. (The exponent of an abelian group is the least common multiple of the orders of the group elements.)

Theorem 4. *If the (not necessarily abelian) group G has a near-factorization $G - e = ST$ and if $\widehat{\ } : G \rightarrow H$ is a homomorphism of G onto an abelian group H of exponent 2, 3, 4 or 6, then there is an element $h \in H$ and positive integers s,t such that $\widehat{S} = sH \pm h$ and $\widehat{T} = tH \mp h^{-1}$. In particular, $|S| \equiv \pm 1 \pmod{|H|}$.*

Proof: Regarding S,T as members of $\mathbb{Z}G$, we get $AB = kH - e$ where $A = \widehat{S}$, $B = \widehat{T}$, and $k = |G|/|H|$. Let $\chi : H \rightarrow \mathbf{C}$ be an irreducible character of H. Extending χ to $\chi : \mathbb{Z}H \rightarrow \mathbf{C}$, we have

$$\chi(A)\chi(B) = k\chi(H) - 1 = -1 \text{ if } \chi \neq \iota \tag{3}$$

where ι is the trivial character, $\iota(h) = 1$ for all $h \in H$.

By the assumption on H, $\chi(A)$ is an integral linear combination of 2, 3, 4 or 6^{th} roots of unity. If ω is any such root, then $\omega + \overline{\omega}$ is an integer. Thus $|\chi(A)|^2 = \chi(A)\overline{\chi(A)}$ is a positive integer as is $|\chi(B)|^2$. So by (3), $\chi(A)\overline{\chi(A)} = 1$ for $\chi \neq \iota$. Thus $\chi(A\overline{A}) = 1$ for $\chi \neq \iota$. If $q = (|A|^2 - 1)/|H|$, then $\chi(A\overline{A} - qH - e) = 0$ for all χ. (Here, we temporarily work in $\mathbf{Q}H$.) Therefore $A\overline{A} = qH + e$. Letting $A = \sum_g a_g g$, where the sum is taken over all $g \in H$, this implies that

$$\sum_g (a_g - a_{kg})^2 = \sum_g a_g^2 - 2(\sum_g a_g a_{kg}) + \sum_g a_{kg}^2 = (q+1) - 2q + (q+1) = 2$$

for each $e \neq k \in H$. Since the coefficients $a_g, g \in H$ are integers, it follows that all but one of them are equal and the remaining coefficient differs from the others by ± 1. Thus $\widehat{S} = A = sH \pm h$ for some integer s and some element $h \in H$. In particular, $|S| = |\widehat{S}| = s|H| \pm 1 \equiv \pm 1 \pmod{|H|}$. It now follows directly that $\widehat{T} = B = tH \mp h^{-1}$ where $|T| = t|H| \mp 1$. ∎

Corollary 2. *If G has a near-factorization $G - e = ST$ and $\widehat{\ }: G \to H$ is a homomorphism of G onto an abelian group H of exponent 2, 3, 4 or 6, then $|S| \geq |H| - 1$.*

Example 7: Taking $G = H$ in Corollary 2, we see that none of the groups C_2^n, C_3^n, C_4^n, $C_2^n \times C_3^m$, $C_2^n \times C_4^m$ has a near-factorization. (This can also be seen using Theorem 3.)

Example 8: Taking $H = C_2^2 \times C_3$, we see from Corollary 2 that $C_2^2 \times C_9$ has no near-factorization since $36 - 1 = 5 \times 7$ and $5 < |H|$. Similarly, none of the following groups has a near-factorization:

$$C_2 \times C_4 \times C_7, C_2^2 \times C_{16}, C_4 \times C_{16}, C_8 \times C_8, C_2 \times C_3 \times C_{16}, C_3 \times C_4 \times C_8.$$

Example 9: For each of the three groups G below, let $\widehat{\ }$ be a homomorphism onto the group H indicated. If any of the groups G had a near-factorization ST with the specified value of $|S|$, then Theorem 4 would imply that $\widehat{S} = H - h$ and $\widehat{T} = H + h^{-1}$ for some $h \in H$:

(i) $G = C_2 \times C_{32}, H = C_2 \times C_4, |S| = 7$,
(ii) $G = C_9 \times C_9, H = C_3 \times C_3, |S| = 8$,
(iii) $G = C_3 \times C_{27}, H = C_3 \times C_3, |S| = 8$.

The next proposition implies that none of the groups in Example 9 has a near-factorization.

Proposition 5. *Let $G - e = ST$ be a near-factorization of an abelian group G. Suppose that there is a homomorphism $\widehat{\ }$ from G onto a group H of order m such that $\widehat{S} = H - e$ and $\widehat{T} = H + e$. Then the powers $g^m, g \in S$ are distinct. In particular, $\{g^m : g \in G\}$ has at least $|S|$ distinct elements.*

Proof: Note that $|H| = m$, $|S| = m - 1$, $|T| = m + 1$ and $|G| = m^2$. In the notation of Proposition 4, the conditions imply that

$$S = \sum_{h \neq e} s(h) \text{ and } T = a + b + \sum_{h \neq e} t(h)$$

where $\widehat{s(h)} = \widehat{t(h)} = h$ for each $e \neq h \in H$, and $\widehat{a} = \widehat{b} = e$. If N is the kernel of the homomorphism, then $|N| = m$ and $G = N + \sum_{h \neq e} s(h) N$. Partitioning the elements of S and T according to their images in H we get

$$s(h)a + s(h)b + \sum_{k \neq e,h} s(k)t(k^{-1}h) = s(h)N \text{ for each } e \neq h \in H.$$

Since G is abelian, the mapping $\sum a_g g \to \prod (g)^{a_g}$ is a homomorphism from $\mathbb{Z}G$ (as an additive group) onto G. Applying this homomorphism, we get

$$s(h)s(h)ab\prod_{k\neq e,h} s(k)t(k^{-1}h) = s(h)^m\left(\prod_{k\in N} k\right) \text{ for each } e \neq h \in H$$

and so

$$s(h)t(h^{-1})ab\prod_{k\neq e} s(k)t(k^{-1}h) = s(h)^m\left(\prod_{k\in N} k\right) \text{ for each } e \neq h \in H$$

Therefore the elements $s(h^{-1})t(h)s(h)^m$, $e \neq h \in H$ are all equal. Thus, the powers $s(h)^m$, $e \neq h \in H$, must be distinct; otherwise, $s(h)t(k) = s(k)t(h)$ for some $h \neq k$ and so ST could not be a near-factorization. ∎

Our results imply that only three of the non-cyclic abelian groups of order at most 100 could possibly have near-factorizations: $C_2^2 \times C_{19}$, $C_2^2 \times C_{23}$, and $C_2^2 \times C_{25}$. Using Theorem 4 and techniques like those employed in Example 6, we have been able to show that $C_2^2 \times C_{19}$ has no near-factorization.

5. Comparision with the factorization problem

A factorization $G = ST$ of the finite group G is a pair S, T of subsets of G such that every $g \in G$ is uniquely representable as $g = st$ with $s \in S$, $t \in T$. The problem of finding all possible factorizations of a group has been studied by several people; see Sands [7] for the most recent paper and references to earlier work. These authors studied abelian groups exclusively; little is known about factorizations of non-abelian groups. A subset S of G is called *periodic* if $S = gS$ for some $e \neq g \in G$. A group G is called *good* if in every factorization $G = ST$, either S or T must be periodic. It was conjectured for some time that every cyclic group is good; the first counterexample was found by Hajós. The determination of all good abelian groups was completed by Sands around 1960. We would like to suggest that Corollary 1 (every near-factor of a finite abelian group is shift-symmetric) is the appropriate analogue of the periodicity property.

In the case of good abelian groups, Sands gave an algorithm for constructing all factorizations. We ask if something similar can be done for near-factorizations of cyclic groups.

Acknowledgements

The first two authors were supported by NSERC grants URF0038628 and A5134, the last author by NSF grant CCR-8711229. We thank Andrew Granville for his help.

References

1. W.G. Bridges and H.J. Ryser, *Combinatorial designs and related systems*, J. Algebra **13** (1969), 432–446.
2. D. de Caen and D.A. Gregory, *On the decomposition of a directed graph into complete bipartite subgraphs*, Ars Combinatoria **23B** (1987), 139–146.
3. A. Granville and M.B. Monagan, *The first case of Fermat's last theorem is true for prime exponents up to 714,591,416,091,389*, Transactions A.M.S. **306, No. 1** (1988), 329–359.
4. C. Lam, *On some solutions of* $A^k = dI + \lambda J$, J. Combin. Th. (A) **23** (1977), 140–147.
5. E.S. Lander, "Symmetric Designs: An Algebraic Approach", Cambridge University Press, Cambridge, 1983.
6. D.A. Marcus, "Number Fields", Springer-Verlag, New York, 1977.
7. A.D. Sands, *On the factorisation of finite abelian groups II*, Acta. Math. Acad. Sci. Hungar. **13** (1962), 153–159.
8. S. Sehgal, "Topics on Group Rings", Dekker, New York, 1987.