J. Algebra Comb. Discrete Appl.
5(1) • 45–49

Received: 11 February 2017
Accepted: 1 September 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

No MacWilliams duality for codes over nonabelian groups

Research Article

M. Ryan Julian Jr.

Abstract: Dougherty, Kim, and Solé [3] have asked whether there is a duality theory and a MacWilliams formula for codes over nonabelian groups, or more generally, whether there is any subclass of nonabelian groups which have such a duality theory. We answer this in the negative by showing that there does not exist a nonabelian group G with a duality theory on the subgroups of G^n for all n.

2010 MSC: 94B60, 20E15

Keywords: Dual code, Subgroup lattice, MacWilliams identity, Iwasawa group

1. Introduction

For codes over finite fields, $C \subset \mathbb{F}_q^n$, the usual inner product for vectors over $\mathbb{F}_q^n$ produces a well established duality theory between C and $C^\perp = \{x \in \mathbb{F}_q^n | \langle x, c\rangle = 0 \ \forall c \in C\}$. Furthermore, the weight enumerator polynomials for a pair of dual codes are related by the famous MacWilliams identity, which for codes over $\mathbb{F}_2$ takes the form $W(C^\perp; x, y) = \frac{1}{|C|} W(C; y-x, y+x)$. There are a number of generalizations of this result that cover different types of weight enumerators as well as codes over different algebraic objects, including abelian groups. Dougherty, Kim, and Solé [3] asked whether it is possible to extend these results to nonabelian groups. In particular, they asked "Is there a subclass of nonabelian groups for which a duality and a MacWilliams formula exist?"

We will answer this question under the assumption that a code over a group G is defined to be a subgroup of G^n, in analogy to the usual definition of codes over abelian groups. Our approach will refrain from choosing a particular definition of a dual code, and instead we will determine whether any suitable choice exists that can provide a duality satisfying our Definition 2.1. It remains open whether there is some other definition of a code over a group G that might better generalize the existing theory of codes over abelian groups, allowing duality to rely on something other than just the subgroup structure.

When they posed the question, Dougherty, Kim, and Solé [3] had already identified one particular difficulty in finding a duality theory for nonabelian groups. They observed that the subgroups of the

M. Ryan Julian Jr.; University of Wisconsin - Madison, United States (email: mrjulian@math.wisc.edu).

http://dx.doi.org/10.13069/jacodesmath.369864 ISSN 2148-838X

quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ do not form a self-dual subgroup lattice. This group has three subgroups of order 4, namely $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, and $\{\pm 1, \pm k\}$, but only one subgroup of order 2, $\{\pm 1\}$. So if we expect codes over G and their duals to be subgroups of G^n with the property that $|C||C^\perp| = |G|^n$, then we would need to restrict our attention to some subclass of nonabelian groups that does not include the quaternions.

Pursuing this line of thought, instead of looking for an inner product that might produce a duality theory, as is done for finite fields and abelian groups, we focus on the structures of subgroup lattices. If a nonabelian group G is to have a duality theory for the subgroups of G^n, it would be necessary for the subgroup lattice of G^n to be self-dual. Fortunately, subgroup lattices with duals have already been classified. In the 1950's, Suzuki determined which finite solvable groups have duals [6], and Zacher was able to prove ten years later that all finite groups with duals are solvable [7]. We will apply this classification to show that if G is a finite nonabelian group with a self-dual subgroup lattice, then $G \times G$ will not have a self-dual subgroup lattice. As a corollary, there cannot exist any nonabelian finite group G with the property that G^n has a self-dual subgroup lattice for all n. While we can define a code over a nonabelian group G to be a subgroup of G^n, there is no subclass of nonabelian groups that will support a duality theory with this definition.

2. Self-dual subgroup lattices

Since our approach to this problem takes us into the theory of subgroup lattices, we will need to begin with a quick tour through the relevant terminology.

Definition 2.1. *Let $L(G)$ denote the subgroup lattice of a group G. We say G has a dual group $\bar{G}$ if there exists a bijective map $\delta : L(G) \to L(\bar{G})$ such that for all $H, K \in L(G)$, $H \leq K$ if and only if $\delta(K) \leq \delta(H)$.*

We are interested in groups that are self-dual, i.e. groups G with a dual $\bar{G} \cong G$. Observe that if G^n was self-dual, then by defining a code over G to be a subgroup of G^n, the duality map for G^n would take a code C to a dual code $C^\perp$. This is the same arrangement that works to produce dual codes over finite fields and abelian groups, but in those cases the duality map can be produced by appealing to an inner product. Without an inner product structure to fall back on for nonabelian groups, we instead depend on studying the subgroup lattices. We will make use of the classification of finite groups with duals given in Chapter 8 of Schmidt's book on subgroup lattices [5], but the classification requires a bit of specialized terminology.

Definition 2.2. *A finite group G is called a P-group if it is:*

1. *an elementary abelian group of prime power order, or*
2. *a group which can be decomposed as $G = S_p S_q$, where S_p is a p-Sylow subgroup which is an abelian P-group, S_q is a cyclic q-Sylow subgroup of order q, $S_q =< B >$, and for any element A of S_p we have*

$$BAB^{-1} = A^r, \quad r \not\equiv 1, \quad r^q \equiv 1 \pmod{p}.$$

Definition 2.3. *A modular lattice is a lattice that satisfies the condition $x \leq b$ implies $x \vee (a \wedge b) = (x \vee a) \wedge b$ for any lattice element a, where $\vee$ and $\wedge$ are the join and meet operations on the lattice. Groups with modular subgroup lattices are called Iwasawa groups.*

Since p-groups with modular subgroup lattices have already been classified by Iwasawa [4], we will not actually need to work much with this definition, but we include it for completeness.

Definition 2.4. *A Hamiltonian group is a nonabelian group G such that every subgroup of G is normal.*

The smallest example of a Hamiltonian group is the quaternion group of order 8 that we met earlier, and, in fact, Dedekind showed that every Hamiltonian group is the direct product of the quaternion group with some other abelian group [2]. We have already seen that the subgroup lattice of the quaternions is not self-dual. So it is perhaps unsurprising that in our attempts to understand self-dual subgroup lattices we will be applying a theorem [5] that instructs us to focus our attention on non-Hamiltonian groups.

Theorem 2.5. *A finite group G has a dual if and only if G is a direct product of finite coprime groups G_λ such that each G_λ is a P-group or a non-Hamiltonian p-group with a modular subgroup lattice.*

In particular, if G is self-dual, it must satisfy this condition. To use this classification to understand codes over G (e.g. subgroups of G^n), we must understand the direct products of P-groups and of non-Hamiltonian p-groups with modular subgroup lattices with themselves. We will examine these first before tackling the main theorem.

3. Direct products

Lemma 3.1. *If G is a nonabelian P-group, then $G \times G$ is not a P-group.*

Proof. From the definition above, a nonabelian P-group must be the semidirect product of an elementary abelian group of order p^k and a cyclic group of prime order q (along with some additional structure). In particular, $|G| = p^k q$, so $|G \times G| = p^{2k} q^2$. Then $G \times G$ cannot be a P-group, since the order of nonabelian P-groups must be of the form $p^\ell q$ for primes p and q. □

To handle the case where G is a non-Hamiltonian p-group with a modular subgroup lattice, we will apply a theorem of Iwasawa [4].

Theorem 3.2. *If G is a non-Hamiltonian nonabelian p-group with a modular subgroup lattice, then G contains an abelian normal subgroup N such that $G/N =< q >$ is cyclic and for all $n \in N$, $q^{-1}nq = n^{1+p^s}$, where $s \geq 1$ ($s \geq 2$ if $p = 2$).*

In fact, to show that this property cannot hold for both G and $G \times G$, we actually only need an abelian normal subgroup with a cyclic quotient. The further structure described in Iwasawa's theorem is unnecessary for the following lemma.

Lemma 3.3. *If G is a nonabelian group, then G and $G \times G$ cannot both be non-Hamiltonian p-groups with modular subgroup lattices.*

Proof. Suppose that both G and $G \times G$ are non-Hamiltonian p-groups with modular subgroup lattices. Let N be an abelian normal subgroup of $G \times G$ such that $(G \times G)/N$ is cyclic, and let p_1 and p_2 be the standard projections $G \times G \to G$. Observe that if $p_1(N) \neq G$ and $p_2(N) \neq G$, then $(G \times G)/N$ cannot be cyclic, since $(G \times G)/N$ would have a non-cyclic quotient. In particular, since $N \subseteq p_1(N) \times p_2(N)$ and $p_1(N)$ and $p_2(N)$ are normal in G, we have

$$((G \times G)/N) \,/\, ((p_1(N) \times p_2(N))/N) \cong (G \times G)/(p_1(N) \times p_2(N))$$

$$\cong (G/p_1(N)) \times (G/p_2(N)),$$

and since $p_1(N) \neq G$ and $p_2(N) \neq G$, we claim that $(G/p_1(N)) \times (G/p_2(N))$ is not cyclic.

To confirm this claim, we first observe that $G/p_1(N)$ and $G/p_2(N)$ are p-groups of orders p^a and p^b, respectively for some integers a and b. Since $p_1(N) \neq G$ and $p_2(N) \neq G$, we know that $a, b > 0$. Then $(G/p_1(N)) \times (G/p_2(N))$ is a group of order $p^a p^b = p^{a+b}$. Suppose that $g_1 \in G/p_1(N)$ and $g_2 \in G/p_2(N)$ with $|g_1| = p^c$ and $|g_2| = p^d$. Then $(g_1, g_2) \in (G/p_1(N)) \times (G/p_2(N))$ and $|(g_1, g_2)| = lcm(|g_1|, |g_2|) = lcm(p^c, p^d) = p^{\max(c,d)}$. Since $c \leq a$, $d \leq b$, and $a, b > 0$, we have that $p^{\max(c,d)} < p^{a+b}$, so (g_1, g_2) cannot

generate $(G/p_1(N)) \times (G/p_2(N))$. Since no element of $(G/p_1(N)) \times (G/p_2(N))$ can generate the entire group, $(G/p_1(N)) \times (G/p_2(N))$ cannot be cyclic.

So, for some $i \in \{1, 2\}$, $p_i(N) = G$. But this contradicts the existence of such an abelian normal subgroup N, since N was chosen to be abelian while G is nonabelian and abelian groups cannot project onto nonabelian groups. □

There is already a result in the literature [1] that states the following: a nonabelian non-Hamiltonian p-group $P = P_1 \times P_2$ is an Iwasawa group if and only if P_1 and P_2 are Iwasawa and, for $i = 1$ or $i = 2$, P_i is abelian such that $\mathrm{Exp}(P_i) \leq p^s$ and s is the integer that comes from the nonabelian factor P_j for $j \neq i$. Our second lemma would be a direct corollary of this result. Unfortunately, the published proof is incorrect, since after establishing elements of P such that $x_1^k a_1^\ell a_2^\ell = x_1 a_1^{1+p^{s_1}} a_2$, the author claims without any further justification that this implies that either $\ell = 1$ or $\ell = 1 + p^{s_1}$. Without this step, there remains a gap in the published proof, so our proof above can be considered a partial correction of that result.

4. The main theorem

With these lemmas in hand, we are now ready to prove the main theorem.

Theorem 4.1. *If G is a finite nonabelian group with a self-dual subgroup lattice, then $G \times G$ does not have a self-dual subgroup lattice.*

Proof. First, if G is a finite nonabelian group with a self-dual subgroup lattice, then by theorem (2.5) G can be expressed as $G = \bigoplus G_\lambda$, where the G_λ are coprime and each G_λ is either a P-group or a non-Hamiltonian p-group with a modular subgroup lattice. Then $G \times G = \bigoplus (G_\lambda \times G_\lambda)$, and since the $G_\lambda \times G_\lambda$ are still coprime, it suffices to check whether it is possible for each $G_\lambda \times G_\lambda$ to still be a P-group or a non-Hamiltonian p-group with a modular subgroup lattice. By theorem (3.1), we know that this will not work if G_λ is a P-group, and by theorem (3.3), we know that this will also not work if G_λ is a non-Hamiltonian p-group with a modular subgroup lattice. Thus we can conclude that if G is a finite nonabelian group with a self-dual subgroup lattice, then $G \times G$ cannot also have a self-dual subgroup lattice. □

5. Conclusion

This result shows that there does not exist any finite nonabelian group G so that G^n has a duality theory for all n. So if we define a code over a nonabelian group G to be a subgroup of G^n, then our coding theory over nonabelian groups cannot have a MacWilliams-type duality theory, and there is no subclass of nonabelian groups where a duality theory could be recovered.

Some variations of Dougherty, Kim, and Solé's question remain open. For example, one could change our definition so that codes over G are not restricted to be subgroups of G^n, and ask whether some other collection of codes could produce meaningful self-dual lattices. Another possibility would be to relax our demands for the duality map. Although our work goes a long way towards describing the boundary between classes of codes with and without duality, the most general form of Dougherty, Kim, and Solé's question, "Find the largest class of algebraic structures A for which a duality and MacWilliams relations hold" remains a target for future research.

References

[1] J. Chifman, Note on direct products of certain classes of finite groups, Commun. Algebra 37(5) (2009) 1831–1842.
[2] R. Dedekind, Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind, Math. Ann. 48(4) (1897) 548–561.
[3] S. Dougherty, J.-L. Kim, P. Solé, Open problems in coding theory, Contemp. Math. 634 (2015) 79–99.
[4] K. Iwasawa, Über die endlichen Gruppen und die Verbände ihrer Untergruppen, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. 4 (1941) 171–199.
[5] R. Schmidt, Subgroup Lattices of Groups, Walter de Gruyter, Berlin, 1994.
[6] M. Suzuki, On the lattice of subgroups of finite groups, Trans. Amer. Math. Soc. 70(2) (1951) 345–371.
[7] G. Zacher, Caratterizzazione dei gruppi immagini omomorfe duali di un gruppo finito, Rend. Sem. Mat. Univ. Padova 31 (1961) 412–422.