On the size of Boolean combinations of subgroups of finite abelian groups

Christian Herrmann

September 7, 2003

Abstract

The sizes of Boolean combinations of subgroups G_i of a finite abelian group depends only on the Boolean expression, the 0-1-sublattice generated by the G_i, and the size of minimal subquotients from this sublattice. Moreover, they increase, monotonically, with those sizes.

Sizes of definable subsets are valuable model-theoretic invariants. For modules, in view of quantifier elimination (cf [4]), such subsets are Boolean combinations of submodules. Following a suggestion of I.Herzog, we show that, in the finite case, these sizes depend only on the isomorphism type of the sublattice generated by these submodules and, in a monotonic way, the sizes of minimal subquotients from this lattice.

To provide a framework where this can be made precise, let L be a modular lattice of finite length and $P(L)$ its set of prime quotients, i.e. of pairs $a > b$ such that $a > x > b$ for no x. An *egde valuation* ν is a map from $P(L)$ into the natural numbers such that $\nu(a/b) = \nu(c/d)$ whenever $c = a + d$ and $b = ad$ - we write $a + b$ and ab for join and meet in lattices. A *representation* of (L, ν) is a lattice homomorphism ϕ of L into the subgroup lattice of some finite abelian group such that $\phi(0_L) = 0$ and such that the cardinality of the quotient subgroup $\phi(a)/\phi(b)$ is $\nu(a/b)$ for every prime quotient a/b. Let N_L be the set of all ν such that (L, ν) has a representation. Observe that the condition on edge valuations is necessary for representability. Nothing is said about existence of representations - and not much is known.

By a Boolean expression over a set S we understand a term $\beta = \beta(a_1, \ldots, a_n)$ built from elements of S, the binary operation symbols $\wedge$, $\vee$, the unary operation symbol $\neg$, and the constants $0, 1$. Given a map $\phi : S \to \mathcal{P}(G)$ we get a subset $\phi(\beta)$ of G by interpretation in the power set algebra $\mathcal{P}(G)$.

Theorem 1 *For every Boolean expression β over a finite length modular lattice L there is an order preserving function $f_{\beta,L}$ from N_L (with pointwise order) to the natural numbers such that*

$$f_{\beta,L}(\nu) = |\phi(\beta)| \quad \text{for every } \nu \in N_L \text{ and representation } \phi \text{ of } (L,\nu)$$

Proposition 2 *Given a subset $S \subseteq L$ there is a function $f_{S,L}$ from N_L into the natural numbers such that for every representation ϕ of (L,ν)*

$$|\phi(1_L) \setminus \bigcup_{s\in S} \phi(s)| = f_{S,L}(\nu).$$

Proof. Let ϕ be any representation and $G = \phi(1_L) = \phi(\emptyset)$. Inclusion-exclusion yields

$$|\phi(1_L) \setminus \bigcup \phi(S)| = \sum_{X\subseteq S} (-1)^{|X|} |\bigcap \phi(X)| = \sum_{X\subseteq S} (-1)^{|X|} |\phi(\prod X)|,$$

where the $\prod X$ are meets in L. But, for an element a of L and maximal chain $a = a_0 \succ a_1 \ldots \succ a_n = 0$ in $[0,a]$ we have

$$|\phi(a)| = \prod_{i=1}^{n} |\phi(a_{i-1})/\phi(a_i)| = \prod_{i=1}^{n} \nu(a_{i-1}/a_i).$$

Fixing a maximal chain C of L, the Jordan-Hölder Theorem tells that the $\nu(a/b)$ with $a/b \in P(C)$ represent all values of ν. In this sense, $f_{S,L}$ is a polynomial in those $\nu(a/b)$ with each monomial of degree at most the length of L.

Lemma 3 *Let L be a direct product of lattices $L_i, i \in I$, with projection maps π_i. Then there is a 1-1-correspondence $\nu \leftrightarrow (\nu_i \,|\, i \in I)$ between edge valuations of L and of the L_i given by $\nu(a/b) = \nu_i(\pi_i a/\pi_i b)$ where i is the unique index with $\pi_i a > \pi_i b$. Moreover*

$$f_{S,L}(\nu) = \prod_{i\in I} f_{S_i,L_i}(\nu_i) \quad \text{where } S_i = \pi_i(S).$$

Proof. With the central elements $z_i = (0, \ldots, 1_i, \ldots, 0)$ we can view the direct decomposition internally: $L_i = [0, z_i]$, $S_i = z_i \cdot S$. In a representation we have

$$\phi(a) = \bigoplus_{i \in I} \phi(z_i a)$$

whence

$$\phi(1_L) \setminus \bigcup \phi(S) = \bigoplus_{i \in I} (\phi(z_i) \setminus \bigcup \phi(S_i)).$$

Lemma 4 *If $S \subseteq M = [z, 1_L]$ and if $z = a_0 \succ a_1 \succ \ldots \succ a_n = 0$ is any maximal chain in $[0, z]$ then*

$$f_{S,L}(\nu) = f_{S,M}(\nu|M) \cdot \prod_{i=1}^{n} \nu(a_{i-1}/a_i).$$

Proof. Of course, any edge valuation can be restricted to any interval sublattice. Inclusion-exclusion and the representation $\phi'(x) = \phi(x)/\phi(z)$ of M in $G/\phi(x)$ provide us with

$$|\phi(1_L) \setminus \bigcup \phi(S)| = \sum_{X \subseteq S} (-1)^{|X|} \bigcap |\phi(X)| = |\phi(z)| (\sum_{X \subseteq S} (-1)^{|X|} \bigcap |\phi(X)/\phi(z)|).$$

Lemma 5 *Let $M = [0, m]$ a lower section of L and S an order ideal of L. Then*

$$f_{S,L}(\nu) = f_{U,L}(\nu) + f_{T,M}(\nu|M) \quad \textit{where } U = S \cup M,\ T = S \cap M.$$

Proof. Observe that $\phi|M$ is a representation of $(M, \nu|M)$ with $m = 1_M$ and that

$$\bigcup \phi(T) = \phi(m) \cap \bigcup \phi(S), \ \ \bigcup \phi(U) = \phi(m) \cup \bigcup \phi(S)$$

$$\phi(1) \setminus \bigcup \phi(S) = (\phi(1) \setminus \bigcup \phi(U)) \uplus (\phi(m) \setminus \bigcup \phi(T).$$

Lemma 6 *Let L be the subspace lattice of an irreducible $n-1$-dimensional projective geometry of order q (i.e. with $q+1$ points on each line). Then $\nu(a/b) = c_\nu$ is constant. If (L, ν) is non-trivially representable, then $c_\nu \geq q$. Moreover,*

$$f_{S,L}(\nu) = \begin{cases} 0 & \textit{if } q^{n-1} \geq c_\nu \\ \prod_{s=0}^{n-1}(c_\nu - q^s) & \textit{else} \end{cases} \qquad S = \{m \in L \mid m \textit{ maximal}\}.$$

Proof. Edge valuations have to be constant: for $a/b \in P(L)$ there is a point p with $a = b + p$, $ap = 0$; and any two points have a common complement. The cases $n = 1, 2$ are obvious. Applying the case $n = 2$ to a line we get $c_\nu \geq q$ in case of nontrivial representability. Now, let $n \geq 3$, ϕ a nontrivial representation and $G = \phi(1_L)$. In particular, ϕ is an embedding. The Arguesian identity of Jónsson [3] holds in the subgroup lattice of G whence in L. It follows that that L is desarguean, i.e. the subspace lattice of some n-dimensional $GF(q)$-vector space V, w.l.o.g. $V = GF(q)^n$. Using e.g. the canonical coordinate system, we have points p of L such that the set $\phi(p)$ is a $GF(q)$-vector space - for an elementary proof see [2]. Hence $c_\nu = q^r$ for some r. Now, by Proposition 2 it suffices to find any G and representation ϕ of (L, ν) and to compute $f_{S,L}$ for that. Such is provided by the tensor product

$$G = GF(c_\nu) \otimes_{GF(q)} V, \quad \phi(U) = GF(c_\nu) \otimes_{GF(q)} U \quad \text{for } U \in L(V).$$

Then $G \cong GF(c_\nu)^n$, canonically, and the $\phi(U)$ are just those subspaces of G which can be defined by equations with coefficients from $GF(q)$. Hence the elements of G not contained in any $\phi(U)$, $U \in L(V)$ maximal, are just the n-tuples of elements of $GF(c)$ linearly independent over $GF(q)$. The number of these is counted by the above formula.

Lemma 7 *Each $f_{S,L}$ is an order preserving function - even stricly increasing except for zero values.*

Proof. Of course,

$$f_{S,L} = f_{\downarrow S,L} \quad \text{where } \downarrow S = \{x \in L \mid \exists s \in S : \ x \leq s\}$$

is the order ideal generated by S in L. We proceed by order induction on the lexicographic combination of the length of L and the corank of $\downarrow S$ in the (distributive) lattice of order ideals of L (i.e. the length of a maximal chain of order ideals of L containing $\downarrow S$) . If $1_L \in S$ then $f_{S,L} \equiv 0$. So let $1_L \notin S$. If $\downarrow S$ is not maximal, then there is an element $m < 1_L$ of L such that $m \notin \downarrow S$ and we can use induction and Lemma 5. Otherwise, we may assume that S consists just of the maximal elements of L. It follows, that $M = [z, 1]$with $z = \prod S$ is complemented ([1] p.88). In view of Lemma 4 we are left to deal with the case where L itself is complemented. But then L is isomorphic to a direct product of irreducible projective geometries (cf [1] p.93). So by Lemma 4 we may assume that L is already such and we are done by Lemma 6.

Observe that the algorithm for computing $f_{S,L}(\nu)$ is polynomial in the size of L and the values of ν.

Proof of the Theorem. We may assume that β is in disjunctive normal form

$$\beta = \bigvee_{\varepsilon \in E} \bigwedge_{i=1}^{n} a_i^{\varepsilon(i)}$$

where E is a set of maps $\varepsilon : \{1, \ldots, n\} \to \{1, -1\}$ and $a^1 = a$, $a^{-1} = \neg a$. Put

$$u_\varepsilon = \prod \{a_i \mid \varepsilon(i) = 1\}, \quad S_\varepsilon = \{u_\varepsilon \cdot a_i \mid \varepsilon(i) = -1\}$$

and let L_ε be the sublattice $[0, u_\varepsilon]$ of L. Then, $\phi(\bigwedge_i a_i^{\varepsilon(i)}) = f_{S_\varepsilon, L_\varepsilon}(\nu | L_\varepsilon)$ and $\phi(u_\varepsilon) \cap \phi(u_\eta) = \emptyset$ for $\varepsilon \neq \eta$ whence $\phi(\beta) = f_{\beta,L}(\nu)$ with

$$f_{\beta,L}(\nu) = \sum_{\varepsilon \in E} f_{S_\varepsilon, L_\varepsilon}(\nu | L_\varepsilon)$$

as required.

References

[1] G.Birkhoff, *Lattice Theory* 3^{rd} *ed.*, AMS Coll. Publ. **25**, Providence R.I. 1967

[2] C.Herrmann, *Frames of permuting equivalences*, Acta Sci.Math. **51** (1987),93-101.

[3] B.Jónsson, *Modular lattices and Desargues' Theorem*, Math.Scand. **2** (1961), 295-314

[4] M.Ziegler, *Model theory of modules*, Ann. Pure Appl. Logic **26** (1984), 149-213

Address

Christian Herrmann, FB Mathematik, Technische Universiät Darmstadt, D64289 Darmstadt, Germany