On constructive recognition of finite simple groups by element orders[1]

A. A. Buturlakin and A. V. Vasil′ev

The set of element orders of a finite group G is called *the spectrum* and denoted by $\omega(G)$, and groups with the same spectrum are said to be *isospectral*. The following question seems to be natural: if $\mathcal{M}$ is a set of positive integers, does a group G with $\omega(G) = \mathcal{M}$ exist, and if so, can one describe all such groups? The paper is concerned with algorithmic aspect of this problem in a special case when G is simple. The following reasons justify the latter restriction. Obviously, there exist non-isomorphic isospectral finite groups, moreover, if G is a finite group with the nontrivial soluble radical, one can construct infinitely many pairwise non-isomorphic finite groups isospectral to G (see, e.g., [1]). On the contrary, in general the set of groups isospectral to a finite nonabelian simple group G is finite and consists of groups closely related to G (see, e.g., [2,3]). Thus, if the name (according to CFSG) of a finite nonabelian simple group G with $\omega(G) = \mathcal{M}$ is determined, then normally the complete list of groups enjoying this property can be achieved.

Note that the spectrum of a group G is closed under taking divisors, i.e., if $n \in \omega(G)$ and d divides n then $d \in \omega(G)$; in particular, $\omega(G)$ is uniquely determined by its subset $\mu(G)$ of elements maximal w.r.t. divisibility. Let $\omega(\mathcal{M})$ and $\mu(\mathcal{M})$ stand respectively for the set of all divisors of elements of $\mathcal{M}$ and the set of all elements of $\mathcal{M}$ maximal w.r.t. divisibility. If we require $\omega(G) = \omega(\mathcal{M})$ instead of $\omega(G) = \mathcal{M}$, then we get the more natural problem whose solution obviously implies a solution of the original problem.

Given a finite group G, the set $\mathcal{M}$ is called *almost G-spectral*, if $\mathcal{M} \subseteq \omega(G)$, $\max \mathcal{M} = \max \omega(G)$, and $\omega(H) \neq \omega(\mathcal{M})$ for every simple group H whose spectrum differs from the spectrum of G. Observe that if G and H are two non-isomorphic finite simple group, then $\omega(G) \neq \omega(H)$ except the cases $\{G, H\} = \{O_8^+(2), S_6(2)\}$ and $\{G, H\} = \{O_8^+(3), O_7(3)\}$ [4]. Therefore, if for a finite set $\mathcal{M}$, we denote by $\Omega(\mathcal{M})$ the set of all simple groups G such that $\mathcal{M}$ is almost G-spectral, then $\Omega(\mathcal{M})$ is either empty, or a singleton, or equal to $\{O_8^+(2), S_6(2)\}$ or $\{O_8^+(3), O_7(3)\}$.

Theorem. *Let $\mathcal{M}$ be a finite set of positive integers, $m = |\mathcal{M}|$ and $M = \max \mathcal{M}$. Then, given $\mathcal{M}$, the set $\Omega(\mathcal{M})$ can be constructed in time polynomial*

[1]The work is supported by Russian Science Foundation (project 14-21-00065).

in $m \log M$*.*

The key tool in our proof is the notion of $\mathcal{M}$-*graph*.

Definition. *Let* $\mathcal{M}$ *be a finite set of positive integers. Given a nonempty subset* $\mathcal{S}$ *of* $\mu(\mathcal{M})$*, define* $v = v(\mathcal{S})$ *to be the greatest positive integer such that* v *divides every element of* $\mathcal{S}$ *and is coprime to every element of* $\mu(\mathcal{M}) \setminus \mathcal{S}$*. Set* $V(\mathcal{M}) = \{v(\mathcal{S}) > 1 \mid \varnothing \neq \mathcal{S} \subseteq \mu(\mathcal{M})\}$ *and refer to elements of* $V(\mathcal{M})$ *as* $\mathcal{M}$*-divisors. The* $\mathcal{M}$*-graph* $\Gamma(\mathcal{M})$ *is the graph with the vertex set* $V(\mathcal{M})$*, and two distinct vertices* v_1 *and* v_2 *are adjacent if and only if* $v_1 v_2 \in \omega(\mathcal{M})$*. For a finite group* G*, we define* $\Gamma(G) = \Gamma(\mu(G))$ *and refer to it as* $\mu(G)$*-graph.*

The $\mathcal{M}$-graph can be constructed inductively, for if $\mathcal{S} \subset \mu(\mathcal{M})$ and $b \in \mu(\mathcal{M}) \setminus \mathcal{S}$, then the vertex sets of $\Gamma(\mathcal{S} \cup \{b\})$ and $\Gamma(V(\mathcal{S}) \cup \{b\})$ coincide. An assumption that $\mathcal{M} \subseteq \omega(G)$ for some simple group G allows to terminate the inductive construction if the $\mathcal{M}$-graph is becoming too large. Therefore, either the size of $\Gamma(\mathcal{M})$ is bounded by polynomial in $\log M$, or $\Omega(\mathcal{M})$ is empty and this can be determined in time bounded by polynomial in $m \log M$.

The graph $\Gamma(G)$ shares some of substantial features with the so-called prime graph $GK(G)$ (see, e.g., [5]) and, as the latter one, reflects essential properties of a simple group G. Using these properties and the assumption that $\Gamma(\mathcal{M}) = \Gamma(G)$, we are able to determine the set $\Omega(\mathcal{M})$ in time polynomially bounded in terms of $m \log M$.

Unfortunately, the fact that $\mathcal{M}$ is almost G-spectral for some simple group G does not imply that $\omega(G) = \omega(\mathcal{M})$. However, if $G \in \Omega(\mathcal{M})$, then our theorem yields that the equality $\omega(G) = \omega(\mathcal{M})$ follows if, given a name of a group G, one is able to construct some set $\nu(G)$ satisfying $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$ and verify that $\nu(G) \subseteq \omega(\mathcal{M})$. Clearly, the time required for this verification is bounded by polynomial in $k \log M$, where $k = |\nu(G)|$. Consulting the description of spectra of simple groups (see, e.g., [6, 7] for the case of classical groups), one may construct some set $\nu(G)$ for every simple group G. The question whether the cardinality of this set can be bounded polynomially in terms of m remains open.

References

1. *V. D. Mazurov*, Recognition of finite groups by a set of orders of their elements, Algebra and Logic, **37**, No. 6 (1998), 371—379.

2. *V. D. Mazurov*, Groups with a prescribed spectrum, Izv. Ural. Gos. Univ. Mat. Mekh., **36** (2005), 119—138.

3. *M. A. Grechkoseeva, A. V. Vasil′ev*, On the structure of finite groups isospectral to finite simple groups (2014), arXiv:1409.8086.

4. *A. A. Buturlakin*, Isospectral finite simple groups, Sib. Élektron. Mat. Izv., **7** (2010), 111—114.

5. *A. V. Vasil'ev, E. P. Vdovin*, An adjacency criterion for the prime graph of a finite simple group, Algebra Logic, **44**, No. 6 (2005), 381—406.

6. *A. A. Buturlakin*, Spectra of finite linear and unitary groups, Algebra Logic, **47**, No. 2 (2008), 91—99.

7. *A. A. Buturlakin*, Spectra of finite symplectic and orthogonal groups, Siberian Adv. Math., **21**, No. 3 (2011), 176—210.

Buturlakin Alexandr Alexandrovich, buturlakin@math.nsc.ru
Sobolev Insitute of Mathematics, 4 Acad. Koptyug avenue, 630090 Novosibirsk Russia
Novosibirsk State University, 2 Pirogova Str., 630090 Novosibirsk Russia

Vasil′ev Andrey Viktorovich, vasand@math.nsc.ru
Sobolev Insitute of Mathematics, 4 Acad. Koptyug avenue, 630090 Novosibirsk Russia
Novosibirsk State University, 2 Pirogova Str., 630090 Novosibirsk Russia