Journal of Combinatorial Theory, Series A 118 (2011) 341–349

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Computational complexity of reconstruction and isomorphism testing for designs and line graphs

Michael Huber [1]

Wilhelm-Schickard-Institute for Computer Science, University of Tuebingen, Sand 13, D-72076 Tuebingen, Germany

ARTICLE INFO

Article history:
Received 12 August 2009

Keywords:
Computational complexity
Reconstructibility
Isomorphism testing
Combinatorial design
Line graph
Graph isomorphism problem
Hypergraph isomorphism problem

ABSTRACT

Graphs with high symmetry or regularity are the main source for experimentally hard instances of the notoriously difficult graph isomorphism problem. In this paper, we study the computational complexity of isomorphism testing for line graphs of t-(v,k,λ) designs. For this class of highly regular graphs, we obtain a worst-case running time of $O(v^{\log v+O(1)})$ for bounded parameters t, k, λ.

In a first step, our approach makes use of the Babai–Luks algorithm to compute canonical forms of t-designs. In a second step, we show that t-designs can be reconstructed from their line graphs in polynomial-time. The first is algebraic in nature, the second purely combinatorial. For both, profound structural knowledge in design theory is required. Our results extend earlier complexity results about isomorphism testing of graphs generated from Steiner triple systems and block designs.

1. Introduction

The Graph Isomorphism (GI) problem consists in deciding whether two given finite graphs are isomorphic – that is, whether there exists an edge-preserving bijection between the vertex sets of the graphs. Besides of its practical importance, the inability to directly classify the GI problem into either of the conventional complexity classes P or NP-complete until now have made it one of the central topics in structural complexity theory. Consequently, it is of interest to identify the difficult instances of the problem.

E-mail address: michael.huber@uni-tuebingen.de.

[1] The author gratefully acknowledges support by the Deutsche Forschungsgemeinschaft (DFG) via a Heisenberg grant (Hu954/4) and a Heinz Maier-Leibnitz Prize grant (Hu954/5).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2010.06.006

The best worst-case algorithm for arbitrary graphs with v vertices has running time $\exp(O(\sqrt{v \log v}))$, see [5,6]. This has mainly been achieved by a combination of Luks' seminal polynomial-time algorithm for graphs of bounded degree [29], together with a combinatorial degree reduction due to Zemlyachenko et al. [42]. After a quarter-century, this moderately exponential bound for graph isomorphism still remains the state of the art despite extensive efforts.

Apparently, many graphs that seem to capture much of the computational difficulty are obtained from highly regular combinatorial structures, like combinatorial designs and related configurations, see [16,31]. Hence, it is a primary goal to reduce for these types of graphs the leading $\sqrt{v}$ term in the exponent to $v^{1/2-\epsilon}$ for some constant $\epsilon > 0$. For important special cases, that of strongly regular graphs and that of line graphs derived from Steiner 2-designs, Spielman [40] reduced the exponent of the exponent to $1/3$ and $1/4$, respectively. For the former, Babai [2] had initially given an elementary combinatorial algorithm in $v^{O(\sqrt{v} \log v)}$ time. Far more efficient isomorphism tests (polynomial-time or even better) are known for several parameterized classes with bounded values for their parameters. The most prominent classes are planar graphs, graphs of bounded degree, bounded genus, bounded color class, or bounded eigenvalue multiplicity. For a unifying treatment of these parameterized classes, see [17]. A strict generalization of the results for bounded degree and bounded genus was obtained in [33,34]. On the other hand, GI-completeness (i.e. there exists a polynomial-time Turing reduction from the GI problem) has been proved for a number of restricted graph classes, including regular graphs, bipartite graphs, chordal graphs, self-complementary graphs, split graphs, and perfect graphs (cf. [42] for some further classes).

In this paper, we consider the computational problem of testing isomorphism of line graphs derived from t-(v, k, λ) designs. For bounded parameters t, k, λ, we obtain a sub-exponential algorithm for this important special class of the GI problem. This extends earlier complexity results about isomorphism testing of graphs generated from Steiner triple systems and block designs. Moreover, as t-(v, k, λ) designs can be viewed as k-uniform hypergraphs on v vertices, this problem is also interesting in view of the recent moderately exponential bound for hypergraph isomorphism: Babai and Codenotti [4] have shown that isomorphism of hypergraphs of bounded rank with v vertices can be tested in time $\exp(\widetilde{O}(\sqrt{v}))$ (where, as usual, the $\widetilde{O}$-notation suppresses polylogarithmic factors).

We state our main result:

Main Theorem. *Isomorphism of line graphs of t-(v, k, λ) designs can be determined in $O(v^{\log v + O(1)})$ time for bounded parameters t, k, λ.*

In a first step, our approach makes use of the Babai–Luks algorithm to compute canonical forms of t-designs. In a second step, we show that t-designs can be reconstructed from their line graphs in polynomial-time. The first is algebraic in nature, the second purely combinatorial. For both, profound structural knowledge in design theory is required. Specifically, we make use of the Ray-Chauduri–Wilson theorem on the minimal number of blocks, an extension of the Erdős–Ko–Rado theorem to t-designs due to Rand, as well as a recent result of Kreher and Rees concerning the maximal size of a subdesign in a t-design.

Related work. There are only a few known complexity results about isomorphism problems related to combinatorial t-designs: Prior to Spielman's result for Steiner 2-designs, Miller [32] had shown that the specific case of isomorphism of line graphs derived from Steiner triple systems (i.e. Steiner 2-designs with block size 3) can be determined in sub-exponential, $O(v^{\log v + O(1)})$, time. His proof uses the fact that a Steiner triple system can be represented as a quasigroup, and hence has a set of at most $1 + \log v$ generators. He also obtained the same bound for testing isomorphism of graphs from Latin squares. Moreover, he gave an $O(v^{\log \log v + O(1)})$ isomorphism algorithm for affine and projective planes. Miller's algorithm has been applied by M. Colbourn [13] to perform isomorphism of Steiner t-designs with block size $t+1$ in $O(v^{\log v + O(1)})$ time. Concerning isomorphism testing of block designs (i.e. 2-designs with arbitrary λ), Babai and Luks [6] derived as a consequence of Luks' techniques [29] an algorithm for bounded block size k and bounded λ in time $O(v^{\log v + f(k,\lambda)})$. On the other hand, C. Colbourn and M. Colbourn [10] verified that the isomorphism problem for block designs is GI-complete, even for triple systems. For a few other results regarding specific designs, we

refer to the survey [14, Sect. 3]. We note that the complexity of the Steiner t-design isomorphism problem in relation to the GI problem is still unresolved (even for fixed t). This is also the case for the isomorphism problem of Steiner triple and quadruple systems, respectively.

Overview. Relevant definitions and concepts from combinatorial design theory including line graphs will be summarized in Section 2. The reader may want to skim this section and return to it when necessary. In Section 3, we apply the Babai–Luks algorithm to compute canonical forms of t-designs. In Section 4, we show that t-designs can be reconstructed from their line graphs in polynomial-time. We finally combine the results of these sections to prove our main theorem.

For further detailed discussion in particular on the GI problem, we refer to the excellent literature: the books by Hoffmann [19], Köbler, Schöning and Torán [26] as well as the surveys by Arvind and Torán [1], Babai [3], Booth and Colbourn [8], Goldberg [18], Köbler [25], Read and Corneil [38], and Zemlyachenko et al. [42]. The current standard reference on the complexity of group-theoretic computation is Seress [39].

2. Designs and line graphs

Combinatorial designs. Combinatorial design theory is a rich subject on the interface of several disciplines, including coding and information theory, cryptography, combinatorics, group theory, and geometry. In particular, the study of designs with high symmetry properties has a very long history and establishes deep connections between these areas (see, e.g., [12,15,20–23,30]).

For positive integers $t \leqslant k \leqslant v$ and λ, we define a t-(v,k,λ) *design* to be a finite incidence structure $\mathcal{D} = (X, \mathcal{B}, I)$, where X denotes a set of *points*, $|X| = v$, and $\mathcal{B}$ a set of *blocks*, $|\mathcal{B}| = b$, satisfying the following regularity properties: each block $B \in \mathcal{B}$ is incident with k points, and each t-subset of X is incident with λ blocks. A *flag* of $\mathcal{D}$ is an incident point-block pair $(x, B) \in I$ with $x \in X$ and $B \in \mathcal{B}$. If $t < k < v$ holds, then we speak of a *non-trivial* t-design. In this paper, 'repeated blocks' are not allowed, that is, the same k-element subset of points may not occur twice as a block. Thus, alternatively a t-(v,k,λ) design can be viewed as a k-uniform hypergraph on v vertices with the property that every set of t vertices is contained in λ common edges.

Incidence preserving maps which take points to points and blocks to blocks are of fundamental importance. We recall the formal definition of an isomorphism between incidence structures: Let $\mathcal{S}_1 = (X_1, \mathcal{B}_1, I_1)$ and $\mathcal{S}_2 = (X_2, \mathcal{B}_2, I_2)$ be two incidence structures. A bijective map

$$\alpha : X_1 \cup \mathcal{B}_1 \longrightarrow X_2 \cup \mathcal{B}_2$$

is an *isomorphism* of $\mathcal{S}_1$ onto $\mathcal{S}_2$, if the following holds:

(i) for $x \in X_1$ and $B \in \mathcal{B}_1$, we have $x^\alpha \in X_2$ and $B^\alpha \in \mathcal{B}_2$,
(ii) for all $x \in X_1$ and all $B \in \mathcal{B}_1$, we have

$$(x, B) \in I_1 \quad \Longleftrightarrow \quad \left(x^\alpha, B^\alpha\right) \in I_2.$$

In this case, the incidence structures $\mathcal{S}_1$ and $\mathcal{S}_2$ are *isomorphic*. An isomorphism of an incidence structure $\mathcal{S}$ onto itself is called an *automorphism* of $\mathcal{S}$. The full group of automorphisms of an incidence structure $\mathcal{S}$ will be denoted by $\mathrm{Aut}(\mathcal{S})$.

For historical reasons, a t-(v,k,λ) design with $\lambda = 1$ is called a *Steiner t-design* (sometimes also a *Steiner system*). The special case of a Steiner design with parameters $t = 2$ and $k = 3$ is called a *Steiner triple system* $\mathrm{STS}(v)$ of order v. A Steiner design with parameters $t = 3$ and $k = 4$ is called a *Steiner quadruple system* $\mathrm{SQS}(v)$ of order v. For example if we consider Steiner quadruple systems, the vector space $\mathbb{Z}_2^d$ with the set $\mathcal{B}$ of blocks taken to be the set of all subsets of four distinct elements of $\mathbb{Z}_2^d$ whose vector sum is zero, is a boolean $\mathrm{SQS}(2^d)$. More geometrically, these $\mathrm{SQS}(2^d)$ consist of the points and planes of the d-dimensional binary affine space $AG(d, 2)$.

By a well-known result of Hanani, a necessary and sufficient condition for the existence of a $\mathrm{SQS}(v)$ is that $v \equiv 2$ or $4 \pmod 6$. For $v = 8$ and $v = 10$ there exists a $\mathrm{SQS}(v)$ in each case,

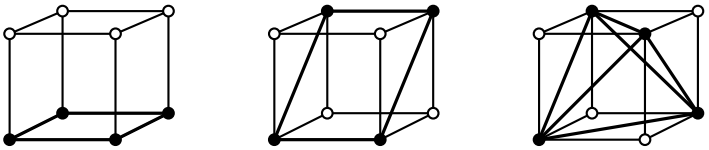

Fig. 1. Illustration of the unique SQS(8), with three types of blocks: faces, opposite edges, and inscribed regular tetrahedra.

unique up to isomorphism. These are the affine space $AG(3,2)$ (cf. Fig. 1) and the Möbius plane of order 3. For $v = 14$ there are exactly 4, and for $v = 16$ exactly 1,054,163 distinct isomorphism types. Lenz [28] proved that for admissible values v, the number $N(v)$ of non-isomorphic SQS(v) grows exponentially, i.e.

$$\liminf_{v\to\infty} \frac{\log N(v)}{v^3} > 0.$$

For a detailed treatment of combinatorial designs, we refer the reader to the encyclopedic accounts [7,11].

We provide some combinatorial tools which will be helpful for the remainder of the paper. For the existence of t-designs, the following basic necessary conditions can be obtained via elementary counting arguments (see, for instance, [7]):

Lemma 1. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a t-(v, k, λ) design, and for a positive integer $s \leqslant t$, let $S \subseteq X$ with $|S| = s$. Then the number of blocks incident with each element of S is given by*

$$\lambda_s = \lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

In particular, for $t \geqslant 2$, a t-(v, k, λ) design is also an s-(v, k, λ_s) design.

It is customary to set $r := \lambda_1$ denoting the number of blocks incident with a given point.

Lemma 2. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a t-(v, k, λ) design. Then the following holds*:

(a) $bk = vr$.
(b) $\binom{v}{t}\lambda = b\binom{k}{t}$.
(c) $r(k-1) = \lambda_2(v-1)$ *for* $t \geqslant 2$.

Lemma 3. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a t-(v, k, λ) design. Then*

$$\lambda\binom{v-s}{t-s} \equiv 0 \left(\mathrm{mod}\ \binom{k-s}{t-s}\right)$$

for each positive integer $s \leqslant t$.

A generalized version of *Fisher's Inequality* for t-designs by Ray-Chaudhuri and Wilson [37, Thm. 1] gives lower bounds on the number of blocks:

Theorem 4 *(Ray-Chaudhuri and Wilson, 1975). Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a t-(v, k, λ) design. If t is even, say $t = 2s$, and $v \geqslant k + s$, then $b \geqslant \binom{v}{s}$. If t is odd, say $t = 2s + 1$, and $v - 1 \geqslant k + s$, then $b \geqslant 2\binom{v-1}{s}$.*

Line graphs. For an incidence structure $\mathcal{S} = (X, \mathcal{B}, I)$, the *line graph* $G(\mathcal{S})$ of $\mathcal{S}$ has as set of vertices the set $\mathcal{B}$ of blocks, whereas any two vertices are adjacent if and only if their corresponding blocks are incident with at least one common point. Line graphs of incidence structures are sometimes

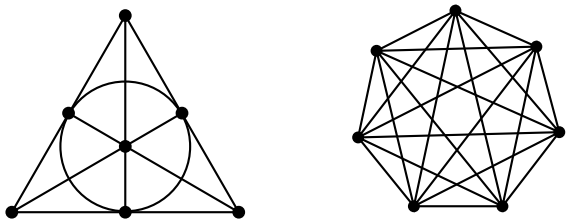

Fig. 2. The Fano plane $PG(2,2)$, and its line graph K_7.

alternatively called *block graphs* or *block intersection graphs* (or *Steiner graphs* in the case of Steiner t-designs). As an example, we consider a Steiner 2-$(7,3,1)$ design, the well-known *Fano plane*, which is the smallest design arising from a finite projective geometry. Since any two of its seven blocks have a point in common, its line graph is isomorphic to the complete graph K_7 (see Fig. 2). We note that a line graph of a Steiner 2-design is a *strongly regular graph*, i.e. each pair of adjacent vertices has the same number of common neighbors, and each pair of non-adjacent vertices has the same number of common neighbors.

Some further notation. An incidence structure $\mathcal{S}_1 = (X_1, \mathcal{B}_1, I_1)$ is called a *substructure* of an incidence structure $\mathcal{S} = (X, \mathcal{B}, I)$, if the following holds:

(i) $X_1 \subseteq X$ and $\mathcal{B}_1 \subseteq \mathcal{B}$,
(ii) for all $x \in X_1$ and all $B \in \mathcal{B}_1$, we have

$$(x, B) \in I_1 \quad \Longleftrightarrow \quad (x, B) \in I.$$

A *subdesign* of a t-(v,k,λ) design is a substructure of the incidence structure which itself is a t-(w,k,λ) design. The subdesign is *proper* if $w < v$.

A *composition series* for a finite group G is a chain of normal subgroups of the form

$$1 = G^m \lhd \cdots \lhd G^2 \lhd G^1 \lhd G^0 = G,$$

in which the quotients G^i/G^{i+1} are simple groups. The factor groups are the *composition factors* of G. They are independent of the choice of composition series by the Jordan–Hölder theorem. The *composition width* of G, denoted by $\mathrm{cw}(G)$, is defined to be the smallest positive integer n such that every non-Abelian composition factor of G embeds in the symmetric group S_n.

Throughout this paper, logarithms are taken base 2. All other notation is standard.

3. Isomorphism testing of designs

A standard algorithmic approach for testing isomorphism of graphs is to try to assign to each graph a *canonical label* (*canonical form*), so that two graphs are isomorphic if and only if the have the same label. For instance, one could start out by labeling the vertices by their degrees, and then *refine* this labeling by further distinguishing equal labels through other local properties of the vertices. If, after refinement, it is possible to endow a unique label to every vertex, then a canonical label for the graph has been found. This procedure with its numerous variations has provided good algorithms for a variety of special classes of graphs. On the other hand, obstacles may occur if the graphs exhibit a high degree of regularity or symmetry, e.g. for regular graphs or graphs associated with highly regular combinatorial structures. In some cases it is possible to break up the symmetry by *individualizing* particular vertices before endowing them with unique labels. For further details on the different methods used for canonical labeling, we refer to [6,38,41] and [9, Sect. 2].

Particularly important for our purposes, Miller [32] showed that a canonical labeling can be found in $O(v^{\log v + O(1)})$ time for Steiner triple systems. His proof relies on the fact that a Steiner triple system can be represented as a quasigroup, and hence has a set of at most $1 + \log v$ generators. By individualizing these, it is then possible to order in polynomial-time the remaining vertices in

a canonical way. Babai and Luks [6] extended this approach by an algebraization of the problem which involves information about the groups of automorphisms. Applied to 2-designs, they obtained the subsequent result.

Theorem 5 *(Babai and Luks, 1983). Canonical forms (and hence isomorphism testing) for non-trivial* 2-(v,k,λ) *designs can be computed in* $O(v^{\log v+f(k,\lambda)})$ *time. In particular, the time bound is* $O(v^{\log v+O(1)})$ *for bounded parameters* k,λ.

A crucial observation in the Babai–Luks approach is the following well-known fact (see, e.g., [11, Ch. II.1]): If there is a 2-(v,k,λ) design containing a proper 2-(w,k,λ) subdesign, then $v \geqslant (k-1)w+1$. As the set of all subdesigns is closed under intersection, any subset 'generates' a subdesign. In order to extend Theorem 5 to t-designs, we need a recent result by Kreher and Rees [27].

Theorem 6 *(Kreher and Rees, 2001). Suppose* $\mathcal{D}$ *is a non-trivial* t-(v,k,λ) *design with* $t \geqslant 2$ *containing a proper* t-(w,k,λ) *subdesign. Then* $v \geqslant 2w$ *when* t *is odd, while* $v \geqslant 2w+1$ *when* t *is even.*

We can now prove the following result.

Theorem 7. *Canonical forms (and hence isomorphism testing) for non-trivial* t-(v,k,λ) *designs with* $t \geqslant 2$ *can be computed in* $O(v^{\log v+f(t,k,\lambda)})$ *time. In particular, the time bound is* $O(v^{\log v+O(1)})$ *for bounded parameters* t, k, λ.

Proof. Let $\mathcal{D}=(X,\mathcal{B},I)$ be a non-trivial t-(v,k,λ) design with $t \geqslant 2$. In view of Theorem 6, we establish the key observation

(1) $\mathcal{D}$ has a generating set S of size at most $1+\log v$.

By individualizing S, we may proceed for the remainder of the proof by straightforwardly adapting the method of proof used for Theorem 5 (cf. [6, Thm. 4.6]). We note that this method relies on results of Luks [29]. In what follows, we describe the basic steps. We first obtain

(2) For fixed t, the composition factors of the setwise stabilizer $\mathrm{Aut}_S(\mathcal{D})$ are subgroups of S_n, where $n=\max(\lambda,k-t)$. In particular, the composition width $\mathrm{cw}(\mathrm{Aut}_S(\mathcal{D}))$ is at most n.

This is then employed in an inductive procedure for finding canonical forms through a nested sequence of graphs. We indicate the underlying construction for the nested graphs. For a sequence $S=(u_1,\ldots,u_s)$, a chain $\{Y_i\}_i$ of subsets of X is constructed as follows: $Y_1=\{u_1\}$ and while $Y_i \neq X$, if Y_i induces a subdesign then $Y_{i+1}=Y_i \cup \{\text{first } u_j \text{ not in } Y_i\}$ else $Y_{i+1}=Y_i \cup \{B \in \mathcal{B}\colon |B \cap Y_i| \geqslant t\}$. The nested graphs $\{H_j\}_j$ are defined as bipartite graphs, H_{2i-1} and H_{2i}, both having the set Y_i on one side and on the other side the vertices representing those blocks entirely in Y_i (for H_{2i-1}) or those in Y_{i+1} (for H_{2i}), and edges correspond to flags. The procedure invokes as a subroutine an algorithm of Babai and Luks (described in detail in [6, Sect. 4.2]) for finding canonical forms for a bipartite graph with respect to a group action on one of its sides, the complexity of which is sensitive to the maximum degree on that side and to the composition width of the group. With respect to the given construction of the nested sequence, it can be shown (again via applying techniques of Luks [29]) that the maximum degree on the side of group action is bounded by $k-t$. We therefore obtain

(3) For fixed t, the total running time is $O(v^{\log v+\omega(\max(\lambda,k-t))+O(1)})$.

This establishes the claim. □

4. Reconstruction of designs from line graphs

If we now give an efficient method of reconstructing a t-design from its line graph, then isomorphism of line graphs of t-(v,k,λ) designs can be tested in $O(v^{\log v+O(1)})$ time for bounded t,k,λ. To accomplish this task, we utilize an extension of the well-known Erdős–Ko–Rado theorem to t-designs, which has been obtained by Rands [36].

Theorem 8. *Let $\mathcal{D}=(X,\mathcal{B},I)$ be a t-(v,k,λ) design. Given $0<s<t\leqslant k$, then there exists a function $f(k,t,s)$ with the following property: suppose there is a subset $\mathcal{A}\subseteq\mathcal{B}$ of blocks such that $|A\cap B|\geqslant s$ for all $A,B\in\mathcal{A}$, then if $v\geqslant f(k,t,s)$, it follows that*

$$|\mathcal{A}|\leqslant\lambda_s \quad (\text{with } \lambda_s \text{ as in Lemma } 1),$$

and the only families of blocks reaching this bound are those consisting of all blocks incident with an s-subset of X.

Furthermore, the function f can be estimated as follows:

$$f(k,t,s)\leqslant\begin{cases} s+\binom{k}{s}(k-s+1)(k-s) & \text{if } s<t-1,\\ s+(k-s)\binom{k}{s}^2 & \text{if } s=t-1.\end{cases}$$

This result will enable us to efficiently find the maximum cliques in a line graph and hence to reconstruct the points of the corresponding t-design. The idea of distinguishing *cliques* (i.e. sets of mutually adjacent vertices) by simple degree considerations, and using the maximum cliques in reconstruction goes back to Miller [32], while retrieving Latin squares, k-nets, and STS(v). It has further been applied by Spielman [40] in case of Steiner 2-designs, and by Östergård et al. [24,35] for STS(v), SQS(v), and Steiner t-designs via Rands' theorem.

We obtain the following result:

Theorem 9. *Let $G(\mathcal{D})$ be a line graph on b vertices derived from a t-(v,k,λ) design $\mathcal{D}$, where $t\geqslant 2$. If $b>k^2(k-1)$, then $\mathcal{D}$ can be reconstructed (up to isomorphism) in time polynomial in b.*

Proof. Let $\mathcal{D}=(X,\mathcal{B},I)$ be a t-(v,k,λ) design with $t\geqslant 2$. Any point $x\in X$ is incident with r distinct blocks. When we consider the line graph $G(\mathcal{D})$ of $\mathcal{D}$, these blocks correspond to vertices in $G(\mathcal{D})$, and x induces edges between all mutual pairs of them. Hence, the blocks intersecting in x define a clique of size r in $G(\mathcal{D})$. Choosing the case $s=1$ in Theorem 8, only this type of clique is of maximum size, if we presume that $v\geqslant f(k,t,1)$. Clearly, for $t\geqslant 2$, always $f(k,t,1)\leqslant 1+k^2(k-1)$, as well as $b\geqslant v$ by Theorem 4. Thus, under the assumption that $b>k^2(k-1)$, we may distinguish algorithmically the maximum cliques and identify them with the points of $\mathcal{D}$ in polynomial time in b. The claim follows. □

We note that $b=\Theta(v^{O(1)})$ for bounded parameters t,k,λ in view of Lemma 2(b).

Remark 10. Spielman [40, Prop. 10] elementary derived the stronger necessary condition $\sqrt{b}-2>(k-1)^2$ in the special case of Steiner 2-designs. We also remark that, in general, reconstructibility from line graphs fails for arbitrary incidence structures. The most natural and oldest graph representation of an incidence structure arguably is by its *point-block incidence graph* (or *Levi graph*). However, this graph representation is normally less compact.

Proof of the Main Theorem. The result is obtained by putting together Theorem 7 and Theorem 9. □

Acknowledgments

I thank Peter Hauck, Michael Kaufmann and Jacobo Torán for interesting discussions about graph isomorphism, and for reading an early draft of this paper. I am also grateful for insightful suggestions from one of the anonymous referees that helped improving the presentation of the paper.

References

[1] V. Arvind, J. Torán, Isomorphism testing: Perspective and open problems, Bull. Eur. Assoc. Theor. Comput. Sci. EATCS 86 (2005) 66–84.
[2] L. Babai, On the complexity of canonical labeling of strongly regular graphs, SIAM J. Comput. 9 (1980) 212–216.
[3] L. Babai, Automorphism groups, isomorphism, reconstruction, in: R.L. Graham, M. Grötschel, L. Lovász (Eds.), Handbook of Combinatorics, vol. II, North-Holland, Amsterdam, New York, Oxford, 1995, pp. 1447–1540.
[4] L. Babai, P. Codenotti, Isomorphism of hypergraphs of low rank in moderately exponential time, in: Proc. 49th Annual IEEE Symposium on Foundations of Computer Science, Philadelphia, PA, 2008, pp. 667–676.
[5] L. Babai, W.M. Kantor, E.M. Luks, Computational complexity and the classification of finite simple groups, in: Proc. 24th Annual IEEE Symposium on Foundations of Computer Science, Tucson, AZ, 1983, pp. 162–171.
[6] L. Babai, E.M. Luks, Canonical labeling of graphs, in: Proc. 15th Annual ACM Symposium on the Theory of Computing, Boston, MA, 1983, pp. 171–183.
[7] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, vols. I and II, Encyclopedia Math. Appl., vol. 69/78, Cambridge Univ. Press, Cambridge, 1999.
[8] K.S. Booth, C.J. Colbourn, Problems polynomially equivalent to graph isomorphism, Technical Report CS-77-04, University of Waterloo, 1979.
[9] J.-Y. Cai, M. Fürer, N. Immerman, An optimal lower bound on the number of variables for graph identification, Combinatorica 12 (1992) 389–410.
[10] C.J. Colbourn, M.J. Colbourn, Concerning the complexity of deciding isomorphism of block designs, Discrete Appl. Math. 3 (1981) 155–162.
[11] C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, second ed., CRC Press, Boca Raton, 2006.
[12] C.J. Colbourn, P.C. van Oorschot, Applications of combinatorial designs in computer science, ACM Comput. Surv. 21 (1989) 223–250.
[13] M.J. Colbourn, An analysis technique for Steiner triple systems, in: Proc. 10th Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, FL, 1979, pp. 289–303.
[14] M.J. Colbourn, Algorithmic aspects of combinatorial designs: A survey, in: C.J. Colbourn, M.J. Colbourn (Eds.), Algorithms in Combinatorial Design Theory, in: Ann. Discrete Math., vol. 26, North-Holland, Amsterdam, New York, Oxford, 1985, pp. 67–136.
[15] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, third ed., Springer, Berlin, Heidelberg, New York, 1998.
[16] D.G. Corneil, C.C. Gotlieb, An efficient algorithm for graph isomorphisms, J. ACM 17 (1970) 51–64.
[17] M. Fürer, Graph isomorphism testing without numerics for graphs of bounded eigenvalue multiplicity, in: Proc. 6th Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco, CA, 1995, pp. 624–631.
[18] M. Goldberg, The graph isomorphism problem, in: J.L. Gross, J. Yellen (Eds.), Handbook of Graph Theory, CRC Press, Boca Raton, 2004, pp. 68–78.
[19] C.M. Hoffmann, Group-Theoretic Algorithms and Graph Isomorphism, Lecture Notes in Comput. Sci., vol. 136, Springer, Berlin, Heidelberg, New York, 1982.
[20] M. Huber, Authentication and secrecy codes for equiprobable source probability distributions, in: Proc. IEEE International Symposium on Information Theory, Seoul, South Korea, 2009, pp. 1105–1109.
[21] M. Huber, Flag-transitive Steiner Designs, Front. Math., Birkhäuser, Basel, Berlin, Boston, 2009.
[22] M. Huber, Combinatorial Designs for Authentication and Secrecy Codes, Foundations and Trends® in Communications and Information Theory, Now Publishers, Boston, Delft, 2010.
[23] M. Huber, Coding theory and algebraic combinatorics, in: I. Woungang, et al. (Eds.), Selected Topics in Information and Coding Theory, World Scientific, Singapore, 2010, pp. 121–158.
[24] P. Kaski, P.R.J. Östergård, The Steiner triple systems of order 19, Math. Comp. 73 (2004) 2075–2092.
[25] J. Köbler, On graph isomorphism for restricted graph classes, in: A. Beckmann, et al. (Eds.), Proc. 2nd Conference on Computability in Europe, Logical Approaches to Computational Barriers, in: Lecture Notes in Comput. Sci., vol. 3988, Springer, Berlin, Heidelberg, New York, 2006, pp. 241–256.
[26] J. Köbler, U. Schöning, J. Torán, The Graph Isomorphism Problem: Its Structural Complexity, Birkhäuser, Basel, Berlin, Boston, 1993.
[27] D.L. Kreher, R.S. Rees, A hole-size bound for incomplete t-wise balanced designs, J. Combin. Des. 9 (2001) 269–284.
[28] H. Lenz, On the number of Steiner quadruple systems, Mitt. Math. Sem. Giessen 169 (1985) 55–71.
[29] E.M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, J. Comput. System Sci. 25 (1982) 42–65.
[30] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, New York, Oxford, 1977, 12. impression 2006.
[31] R.A. Mathon, Sample graphs for isomorphism testing, in: Proc. 9th Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, FL, 1978, pp. 499–517.
[32] G.L. Miller, On the $n^{\log n}$ isomorphism technique: A preliminary report, in: Proc. 10th Annual ACM Symposium on the Theory of Computing, San Diego, CA, 1978, pp. 51–58.
[33] G.L. Miller, Isomorphism of graphs which are pairwise k-separable, Information and Control 56 (1983) 21–33.
[34] G.L. Miller, Isomorphism of k-contractible graphs. A generalization of bounded valence and bounded genus, Information and Control 56 (1983) 1–20.
[35] I.Yu. Mogilnykh, P.R.J. Östergård, O. Pottonen, F.I. Solov'eva, Reconstructing extended perfect binary one-error-correcting codes from their minimum distance graphs, IEEE Trans. Inform. Theory 55 (2009) 2622–2625.
[36] B.M.I. Rands, An extension of the Erdős, Ko, Rado theorem to t-designs, J. Combin. Theory Ser. A 32 (1982) 391–395.

[37] D.K. Ray-Chaudhuri, R.M. Wilson, On t-designs, Osaka J. Math. 12 (1975) 737–744.
[38] R.C. Read, D.G. Corneil, The graph isomorphism disease, J. Graph Theory 1 (1977) 339–363.
[39] A. Seress, Permutation Group Algorithms, Cambridge Univ. Press, Cambridge, 2003.
[40] D.A. Spielman, Faster isomorphism testing of strongly regular graphs, in: Proc. 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, 1996, pp. 576–584.
[41] B. Weisfeiler (Ed.), On Construction and Identification of Graphs, Lecture Notes in Math., vol. 558, Springer, Berlin, Heidelberg, New York, 1976.
[42] V.M. Zemlyachenko, N.M. Kornienko, R.I. Tyshkevich, Graph isomorphism problem, J. Soviet Math. 29 (1985) 1426–1481.