# Applying Combinatorial Techniques To Find Minimal Non-Complete Set Coverings

Enrico Piccione and Jan Vorloeper

Ruhr University Bochum, Bochum, Germany
firstname.lastname@rub.de

**Abstract.** One of the most prominent hardware countermeasures against side-channel attacks are threshold implementations (TIs). The technique uses masking to split the operations in a cryptographic algorithm into several ones operating on shares. The coverage and non-completeness requirements of TIs are mathematically described by the notion of non-complete set coverings (NCSCs). Importantly, the number of members inside an NCSC determines the number of output shares and therefore directly impacts the complexity of the resulting TI.
In this work, we derive new lower bounds on the minimal number of members of NCSCs and obtain new upper bounds by explicit constructions. We present a group-theoretic construction of balanced NCSCs, in which the numbers of input and output shares coincide, together with a search algorithm based on intersections of group translates. Our methods determine the smallest balanced coverings in two previously unresolved cases and yield exact minima and classifications of optimal coverings for an infinite family of parameters. These results resolve all four explicit open problems posed by Farràs, Fidalgo and Lara-Nino.

## 1 Introduction

Side-channel attacks exploit physical leakage of a device, such as its power consumption or electromagnetic emanation, in order to recover secret keys from otherwise secure cryptographic algorithms [KJJ99]. One of the most widely studied countermeasures against side-channel analysis is masking, in which every sensitive intermediate value is split into several randomized shares, so that any small number of shares is independent of the secret. The security of masking schemes is commonly analysed in the $d$-probing model [ISW03], in which an adversary may observe up to $d$ intermediate values of the computation.

In hardware, however, masking alone is not sufficient, as glitches may cause a single gate to leak information about several shares at once. Threshold implementations (TIs), first introduced in [NRR06] and generalized to higher orders in [BGN+14], address this issue by splitting a function into several component functions, each of which depends only on a subset of the $s$ input shares. This property, called non-completeness, guarantees that any $d$ component functions together are independent of at least one input share, so computations confined

to these components are independent of the secret when the input sharing is uniform. In order to implement a Boolean function of algebraic degree $t$ in this way, every monomial must be computable by some component function, i.e. every $t$ input shares must jointly appear in at least one of them. Output uniformity and the conditions for secure composition must be established separately.

Throughout, we define $U_k := \{1, \ldots, k\}$ for any positive integer $k$, and call a subset $T \subseteq U_k$ a $t$-set if $|T| = t$. For a finite set $X$, we write $\binom{X}{t}$ for the family of its $t$-subsets, whose cardinality is $\binom{|X|}{t}$.

**Definition 1.** *Given positive integers $s, t, d, r$ with $s \geq t$, let $\mathcal{C} := (S_i)_{i \in U_r}$ be a family of $r$ subsets $S_i \subseteq U_s$, called the members of $\mathcal{C}$. Then, $\mathcal{C}$ is a* non-complete set covering *(NCSC) of degree $t$ and order $d$, denoted* $\mathrm{nc}(s, t, d, r)$*, if the following conditions hold:*

1. *Every $t$-set $T \subseteq U_s$ satisfies $T \subseteq S_i$ for some $i \in U_r$,*
2. *Every $H \subseteq U_r$ with $|H| \leq d$ satisfies $\bigcup_{i \in H} S_i \neq U_s$.*

*Furthermore, we denote $\rho_{t,d}(s) := \min\{r \mid \mathrm{nc}(s, t, d, r) \text{ exists}\}$.*

Note that this definition differs from those in [Pet19,AZN21,FFL26] as it omits their second condition, enforcing that $|S_i| \geq t$ for all $i \in U_r$. As already stated in the literature, this condition is mainly used to rule out trivially non-minimal coverings, and is not strictly necessary to construct a valid $d$-th order threshold implementation for a Boolean function of algebraic degree $\leq t$. Concretely, removing a member $T$ with $|T| < t$ does not affect any of the conditions of an NCSC, hence yields an $\mathrm{nc}(s, t, d, r - 1)$.

Here, the points correspond to the input shares, and the members of the covering correspond to the component functions, i.e. to the output shares. Since every output share requires its own circuit and the output shares may require refreshing or compression between rounds before they can serve as input to the next round function, the number of members directly impacts the area, randomness and latency of the resulting TI. This motivates the central question of this work, namely to determine the minimal number $\rho_{t,d}(s)$ of members of an NCSC with $s$ points, degree $t$ and order $d$. Of particular practical interest are balanced coverings, i.e. coverings with as many members as points, as they allow the output shares of one round to be reused as input shares of the next round without changing the number of shares.

*Related Work.* Non-complete set coverings were introduced by Petrides [Pet19] to describe the dependence structures of higher-order TIs. Their use in low-latency and high-performance masked implementations has been investigated in [AZN21,GLN25,GL25]. Farràs et al. [FFL26] gave a systematic treatment, including new bounds, a duality between the parameters $t$ and $d$, and tables of the best known coverings for small parameters. Nevertheless, for most parameters $(t, d)$ the exact values of $\rho_{t,d}(s)$ remain unknown.

In the literature, we found two equivalent formulations of NCSCs, in terms of intersecting set families and of bipartite tournaments, both of which have

been studied independently of their application to threshold implementations. Taking complements of the members, an NCSC of order $d$ corresponds to a $d$-wise intersecting family whose transversal number exceeds $t$, a notion going back to [EL75]. Equivalently, in [BGHT03] bipartite tournaments with property $S_{d,t}$ have been studied, which is a bipartite variant of Schütte's tournament problem, and gave probabilistic and geometric constructions. While these constructions apply directly to NCSCs, they do not improve any of the values considered here, as they target the asymptotic behaviour rather than small parameters. The tools used below include Schönheim's recursive bound for coverings [Sch64], results on intersecting triple systems [PR17], and group actions for constructing coverings with prescribed symmetries.

*Our Contribution.* We resolve all four explicit open problems posed in [FFL26], by explicitly constructing $\mathrm{nc}(15, 4, 2, 15)$, $\mathrm{nc}(18, 3, 3, 18)$ and $\mathrm{nc}(19, 3, 3, 19)$, which all attain the known lower bounds on the smallest balanced coverings, and by showing $\rho_{3,2}(8) = 17$, ruling out the existence of $\mathrm{nc}(8, 3, 2, r)$ for $r \leq 16$.

We also give balanced coverings with 34 shares for $(4, 3)$ and $(3, 4)$, and determine $\rho_{3,2}(s)$ and $\rho_{2,3}(s)$ for all $s \geq 7$, as listed in Table 3, as well as $\rho_{4,2}(s)$ for all $s \geq 26$. More generally, we determine $\rho_{2,d}(2d+2)$ and classify its optimal coverings for every $d \geq 3$. The proofs combine counting and duality with results on intersecting families. Table 1 compares these and our other new coverings with the previous upper bounds and our lower bounds.

A central technique which we introduce constructs balanced coverings from all translates $Bg$, $g \in G$, of a single subset $B$ of a finite group $G$. We characterize these coverings through their automorphism groups and give a search algorithm that uses regularity, duality and bounds on intersections of translates to reject candidates early. We complement this approach computationally, by using SAT models with prescribed automorphisms via the Kramer-Mesner formulation, as well as without symmetry assumptions, via simulated annealing. Further coverings arise from duality, from explicit algebraic constructions, and from the structural analysis of the boundary case $s = td + 2$ in Section 4.

All new coverings are available in our GitHub repository.[1]

## 2 New Bounds for Non-Complete Set Coverings

In this section, we derive lower bounds on $\rho_{t,d}(s)$ from the combinatorial structure of non-complete set coverings, recalling known bounds where they apply and complementing them with new ones. Many of these bounds come in pairs, as non-complete coverings are naturally related to coverings with the roles of $t$ and $d$ exchanged, via the notion of duality (first introduced in [FFL26]).

**Lemma 1 (Duality).** *An* $\mathrm{nc}(s, t, d, r)$ *exists iff an* $\mathrm{nc}(r, d, t, s)$ *exists. Explicitly, for* $\mathcal{C} = (S_i)_{i \in U_r}$ *and* $p \in U_s$ *let* $R_p := \{i \in U_r : p \notin S_i\}$ *be the set of indices*

[1] See https://github.com/vorlojan6/list-of-new-ncsc.

| $(t,d)=(4,2)$ | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $s$ | 10 | 11 | 12 | 13 | 14 | 15 | 18 | 22 | 26 | 31 |
| previous [FFL26] | 56 | 37 | 28 | 22 | 18 | 16 | 15 | 15 | 15 | 15 |
| this work | 53 | 33 | 26 | 20 | 17 | **15** | 13 | 12 | 11 | 10 |
| lower bound | 50 | 26 | 19 | 18 | 16 | 12 | 12 | 11 | 11 | 10 |

| $(t,d)=(3,3)$ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $s$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 25 | 26 | 29 | 37 |
| previous [FFL26] | 69 | 56 | 43 | 36 | 30 | 26 | 22 | 20 | 18 | 17 | 17 | 15 |
| this work | 59 | 44 | 37 | 29 | 26 | 25 | **18** | 18 | 17 | 16 | 15 | 14 |
| lower bound | 36 | 32 | 26 | 22 | 20 | 20 | 18 | 18 | 15 | 14 | 14 | 12 |

| $(t,d)=(3,4)$ | | | |
|---|---|---|---|
| $s$ | 26 | 27 | 34 |
| previous [FFL26] | 286 | 286 | 286 |
| this work | 100 | 54 | **34** |
| lower bound | 29 | 27 | 24 |

| $(t,d)=(4,3)$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| $s$ | 20 | 22 | 24 | 25 | 26 | 28 | 34 |
| previous [FFL26] | 715 | 715 | 715 | 715 | 715 | 715 | 715 |
| this work | 171 | 126 | 115 | 96 | 75 | 56 | **34** |
| lower bound | 51 | 38 | 31 | 29 | 29 | 27 | 24 |

**Table 1.** Upper bounds on $\rho_{t,d}(s)$ attained by the new coverings of this work, compared to the best previously known upper bounds [FFL26] and to the lower bounds proved in this paper. For $(3,4)$ and $(4,3)$, the previous values are the trivial bounds $\binom{13}{3}$ and $\binom{13}{4}$. Bold entries are balanced, i.e. $r=s$, and entries where the upper and lower bounds coincide determine $\rho_{t,d}(s)$ exactly. Values for $s$ not listed follow by monotonicity, see Figure 1.

*of the members not containing $p$. Then $\widehat{\mathcal{C}} := (R_p)_{p\in U_s}$ is an* $\mathrm{nc}(r,d,t,s)$ *on the point set $U_r$. We call $\widehat{\mathcal{C}}$ the* dual covering *of $\mathcal{C}$.*

We recall that, unlike the definitions in [Pet19,AZN21,FFL26], our definition permits members of size less than $t$. Such members may be deleted without affecting either condition, so allowing them does not change the minimal number of members. This convention also allows the dual family to be retained without deleting small members. Moreover, when representing coverings $\mathcal{C}$ in terms of their $s\times r$ incidence matrices $(X_{ij}^{(\mathcal{C})})_{i\in U_s, j\in U_r}$ with $X_{ij}^{(\mathcal{C})}=1$ if $i\in S_j$ and zero otherwise, we have $X^{(\widehat{\mathcal{C}})} = J - (X^{(\mathcal{C})})^T$, where $J$ denotes the all-ones matrix of the appropriate dimensions. Note that this immediately proves that taking the dual is an involution:

$$X^{(\widehat{\widehat{\mathcal{C}}})} = J - (J - (X^{(\mathcal{C})})^T)^T = X^{(\mathcal{C})}.$$

For $T\subseteq U_s$ and $H\subseteq U_r$ we write

$$\lambda_{\mathcal{C}}(T) := |\{i\in U_r : T\subseteq S_i\}|, \qquad \mu_{\mathcal{C}}(H) := \Big|U_s \setminus \bigcup_{i\in H} S_i\Big|,$$

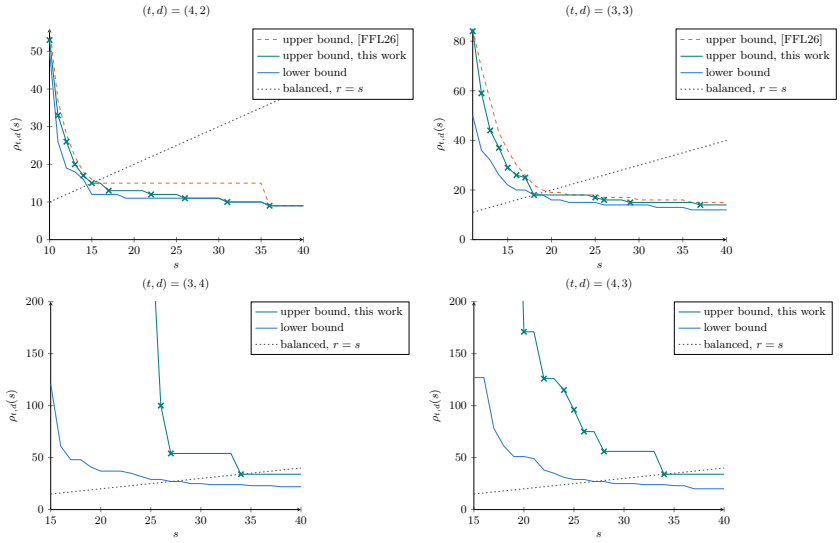


**Fig. 1.** Best known bounds on $\rho_{t,d}(s)$. Dashed orange: upper bounds known before this work, i.e. from [FFL26]. Solid teal: upper bounds of this work, where crosses mark values attained by an explicit covering and the bounds in between follow by monotonicity. For $(3,4)$ and $(4,3)$ no upper bound below the trivial one was published before.

to denote respectively the number of members containing $T$ and the number of points missed by all members indexed by $H$. We moreover denote by $\deg_{\mathcal{C}}(p) := \lambda_{\mathcal{C}}(\{p\})$ the *degree* of a point $p$. All of these count members with multiplicity, and we omit the subscript $\mathcal{C}$ if it is clear from the context.

We continue by recalling a basic existence criterion for non-complete coverings.

**Lemma 2 ([Pet19, Proposition 2.5]).** *An* $\mathrm{nc}(s,t,d,r)$ *exists only if* $s \geq td+1$. *If an* $\mathrm{nc}(s,t,d,r)$ *exists, then an* $\mathrm{nc}(s+1,t,d,r)$ *exists. Hence,* $\rho_{t,d}$ *is non-increasing for* $s \geq td+1$.

Using duality, we can immediately convert that bound to one on $r$.

**Corollary 1.** *Every* $\mathrm{nc}(s,t,d,r)$ *has* $r \geq td+1$. *Moreover, an* $\mathrm{nc}(s,t,d,td+1)$ *exists iff* $s \geq \binom{td+1}{d}$.

*Proof.* By Lemma 2, every $\mathrm{nc}(r,d,t,s)$ has $r \geq dt+1$, so the first statement follows from duality, see Lemma 1.

For the second statement, suppose first that $s \geq \binom{td+1}{d}$. By Lemma 2, it suffices to consider $s = \binom{td+1}{d}$, so we identify the points with the $d$-subsets of $U_{td+1}$, and let $S_i$ consist of all $d$-subsets $D$ with $i \notin D$, for $i \in U_{td+1}$. Any $t$ points $D_1, \ldots, D_t$ satisfy $|D_1 \cup \cdots \cup D_t| \leq td$, so some $i \in U_{td+1}$ lies in none of them, and hence all of them lie in $S_i$. Moreover, any $H \subseteq U_{td+1}$ with $|H| \leq d$

is contained in a $d$-set $D$, and the point $D$ is missed by all members indexed by $H$. Thus $(S_i)_{i\in U_{td+1}}$ is an $\mathrm{nc}(s,t,d,td+1)$.

Conversely, let $\mathcal{C}$ be an $\mathrm{nc}(s,t,d,td+1)$. We first show that every point $p$ satisfies

$$\deg(p) \geq (t-1)d+1. \tag{1}$$

For $t=1$ this follows from the covering property, so let $t\geq 2$. The family $(S_i\setminus\{p\})_{i:p\in S_i}$ on $U_s\setminus\{p\}$ has $\deg(p)$ members. It covers every $(t-1)$-set $A$, since $A\cup\{p\}$ is a $t$-set and lies in some member, which then contains $p$. Moreover, any $d$ of its members miss a common point of $U_s$, which is not $p$, as all of them contain $p$. Thus, it forms an $\mathrm{nc}(s-1,t-1,d,\deg(p))$, and the first statement gives (1). Consequently, every point is missed by $|R_p| = r-\deg(p) \leq td+1-(t-1)d-1 = d$ members.

Now let $H\subseteq U_{td+1}$ with $|H|=d$. By non-completeness, some point $p$ is missed by all members indexed by $H$, i.e. $H\subseteq R_p$, and as $|R_p|\leq d$ we get $R_p = H$. Hence $p\mapsto R_p$ hits every $d$-subset of $U_{td+1}$, and therefore $s\geq \binom{td+1}{d}$. □

Note that the argument in the first step of the converse does not use $r=td+1$. Applied to $\mathcal{C}$ it bounds the degree $\deg(p)$ of every point, and applied to $\widehat{\mathcal{C}}$ it bounds the cardinality of every member.

**Lemma 3 ([FFL26, Theorem 2]).** *In an* $\mathrm{nc}(s,t,d,r)$, $|S_i|\leq s-(d-1)t-1$ *for every* $i\in U_r$. *Moreover, every point has degree at least* $(t-1)d+1$.

*Proof.* The second statement is the first step of the converse in the proof of Corollary 1. Applying it to $\widehat{\mathcal{C}}$, every member of $\mathcal{C}$ is missed by at least $(d-1)t+1$ points, giving the first statement. □

More generally, restricting $\mathcal{C}$ to the members containing a fixed set of points yields a non-complete covering with smaller parameters, which leads to the following generalization of the degree bound in Lemma 3.

**Lemma 4.** *Let* $\mathcal{C}$ *be an* $\mathrm{nc}(s,t,d,r)$, *and let* $T\subseteq U_s$ *with* $|T|=j<t$ *and* $H\subseteq U_r$ *with* $|H|=j<d$. *Then* $\lambda(T)\geq \rho_{t-j,d}(s-j)$ *and* $\mu(H)\geq \rho_{d-j,t}(r-j)$.

*Proof.* The family $\mathcal{C}_T := (S_i\setminus T)_{i\,:\,T\subseteq S_i}$ on $U_s\setminus T$ has $\lambda(T)$ members. Every $(t-j)$-subset $A$ of $U_s\setminus T$ is contained in one of them, since $T\cup A$ is a $t$-set, and any $d$ of them miss a common point of $U_s$, which lies outside $T$, as all of them contain $T$. Hence $\mathcal{C}_T$ is an $\mathrm{nc}(s-j,t-j,d,\lambda(T))$, and $\lambda(T)\geq\rho_{t-j,d}(s-j)$. The second statement follows by applying the first to $\widehat{\mathcal{C}}$, since $\mu_{\mathcal{C}}(H)=\lambda_{\widehat{\mathcal{C}}}(H)$. □

Since $\rho_{t-j,d}(s-j)\geq (t-j)d+1$ by Corollary 1, this generalizes the degree bound of Lemma 3, and it is strictly stronger whenever a better lower bound on $\rho_{t-j,d}(s-j)$ is known. As a concrete example, the lower bounds for $(4,3)$ are derived like this from bounds on $(3,3)$ established in [FFL26].

### 2.1 The Schönheim Bounds

We continue with two further bounds which lower-bound $r$ in terms of $s$ and $m$, the size of the largest member, by counting how often every small set of points must be covered. As it turns out, these are exactly the Schönheim bound for coverings [Sch64], a classical bound from design theory, applied to members of size at most $m$.

**Definition 2.** *Let $\mathcal{C}$ be an $\mathrm{nc}(s,t,d,r)$ whose members have at most $m$ elements. Define*

$$\sigma_t = 1, \text{ and } \sigma_j = \left\lceil \sigma_{j+1} \frac{s-j}{m-j} \right\rceil \text{ for } 1 \le j \le t-1, \tag{2}$$

*as a lower bound on the minimal number of members of $\mathcal{C}$ in which any $j$-set lies. In other words, $\lambda(T) \ge \sigma_j$ for every $j$-set $T \subseteq U_s$, $1 \le j \le t$.*

**Theorem 1 ([FFL26, Theorem 7]).** *Let $t \ge 2$ and let $\mathcal{C}$ be an $\mathrm{nc}(s,t,d,r)$. With $m$ and $\sigma_j$ as in Definition 2, we have*

$$r \ge r_0 := \max_{1 \le j \le t} \left\lceil \sigma_j \binom{s}{j} \Big/ \binom{m}{j} \right\rceil,$$

*and consequently $\rho_{t,d}(s) \ge \min\{r_0 \mid t \le m \le s-(d-1)t-1\}$.*

Similar to before, this bound was already stated in [FFL26], but applying duality yields another bound which is given below.

**Corollary 2.** *Let $\mathcal{C}$ be an $\mathrm{nc}(s,t,d,r)$ with $d \ge 2$, and let $\widehat{m} = \max_p |R_p|$ be the maximal cardinality of a member in $\widehat{\mathcal{C}}$. Dually to above, define*

$$\widehat{\sigma}_d = 1, \text{ and } \widehat{\sigma}_j = \left\lceil \widehat{\sigma}_{j+1} \frac{r-j}{\widehat{m}-j} \right\rceil \text{ for } 1 \le j \le d-1. \tag{3}$$

*Then*

$$s \ge \max_{1 \le j \le d} \left\lceil \widehat{\sigma}_j \binom{r}{j} \Big/ \binom{\widehat{m}}{j} \right\rceil. \tag{4}$$

*Consequently, if an $\mathrm{nc}(s,t,d,r)$ exists, then $s$ is at least the minimum of the right-hand side of (4) for $d \le \widehat{m} \le r-(t-1)d-1$.*

*Proof.* The dual covering $\widehat{\mathcal{C}}$ has $r$ points, degree $d$, order $t$ and exactly $s$ members, and its largest member has $\widehat{m}$ elements, thus applying Theorem 1 to $\widehat{\mathcal{C}}$ gives (4). For the last statement, some $R_p$ contains a $d$-set of indices, so $\widehat{m} \ge d$, and $\widehat{m} \le r-(t-1)d-1$ because every point has degree at least $(t-1)d+1$ by Lemma 3. □

Interestingly, these two bounds can be played against each other, since a bound on the member sizes improves the bound on the sets $R_p$ and vice versa.

**Theorem 2.** *Let $t, d \geq 2$ and let $\mathcal{C}$ be an $\mathrm{nc}(s,t,d,r)$ in which every member has at most $m$ elements and every set $R_p$ has at most $\widehat{m}$ elements, and let $\sigma_j$ and $\widehat{\sigma}_j$ be as in (2) and (3), respectively. Then every member has at most $s-\widehat{\sigma}_1$ elements, and every set $R_p$ has at most $r-\sigma_1$ elements.*

*Proof.* By Theorem 1 every point lies in at least $\sigma_1$ members, so $|R_p| \leq r-\sigma_1$ for every $p$.

For the other statement we show that $\mu(H) \geq \widehat{\sigma}_j$ for every $H \subseteq U_r$ with $|H| = j$ and $1 \leq j \leq d$, which is the non-completeness property for $j = d$.

For $j = d-1$, let $P$ be the set of points that lie in none of the members indexed by $H$, which is nonempty by non-completeness. Suppose that $|P| \leq t$, then $P \subseteq S_i$ for some $i \in U_r$ by the covering property, and $i \notin H$, as the members indexed by $H$ miss $P \neq \varnothing$. Hence the $d$ members indexed by $H \cup \{i\}$ cover $U_s$, contradicting non-completeness, and thus $\mu(H) = |P| \geq t+1$. The counting argument below also applies for $j = d-1$ with $\widehat{\sigma}_d = 1$, giving $\mu(H) \geq \lceil (r-d+1)/(\widehat{m}-d+1) \rceil = \widehat{\sigma}_{d-1}$.

For $j < d-1$, count the pairs $(i,p)$, where $i \in U_r \setminus H$ and $p$ is a point that lies in none of the members indexed by $H \cup \{i\}$. There are $r-j$ choices of $i$, each with at least $\widehat{\sigma}_{j+1}$ points. On the other hand, a point $p$ missed by the members indexed by $H$ is missed by at most $\widehat{m}-j$ further members, since $|R_p| \leq \widehat{m}$. Hence $\mu(H) \geq \widehat{\sigma}_{j+1} \cdot (r-j)/(\widehat{m}-j)$. For $j = 1$, it means that every member is missed by at least $\widehat{\sigma}_1$ points. □

Note that $\sigma_1(m)$ and $\widehat{\sigma}_1(\widehat{m})$ are non-increasing functions in $m$ and $\widehat{m}$, respectively. Hence, every improved bound on $m$ or $\widehat{m}$ obtained from Theorem 2 may again improve the other one, as each application may lower the bounds on $m$ and $\widehat{m}$, which in turn raises $\sigma_1$ and $\widehat{\sigma}_1$ for the next one, until the bounds either stabilise or become contradictory.

**Corollary 3.** *Start with $m_0 = s-(d-1)t-1$ and $\widehat{m}_0 = r-(t-1)d-1$ from Lemma 3 and let*

$$m_{i+1} = \min\bigl\{m_i,\ s-\widehat{\sigma}_1(\widehat{m}_i)\bigr\}, \qquad \widehat{m}_{i+1} = \min\bigl\{\widehat{m}_i,\ r-\sigma_1(m_i)\bigr\}.$$

*Then, if an $\mathrm{nc}(s,t,d,r)$ exists, $m_i \geq t$ and $\widehat{m}_i \geq d$ for all $i$, and the inequalities of Theorem 1 and Corollary 2 hold with $m_i$ and $\widehat{m}_i$ in place of $m$ and $\widehat{m}$.*

*Proof.* By induction and Theorem 2, every member has at most $m_i$ elements and every $R_p$ has at most $\widehat{m}_i$ elements. A member contains a $t$-set and some $R_p$ contains a $d$-set of indices, which gives the first statement. The right-hand sides of the two counting bounds decrease in $m$ resp. $\widehat{m}$, so they remain valid for the upper bounds $m_i$ and $\widehat{m}_i$. □

*Example 1.* As a concrete example, suppose an $\mathrm{nc}(23,4,3,27)$ exists. Here we have $m_0 = 14$ and $\widehat{m}_0 = 17$. For this example, we strengthen the first recursion

steps to

$$\sigma_{t-1} = \max\left\{d+1, \left\lceil \frac{s-t+1}{m-t+1} \right\rceil\right\},$$
$$\widehat{\sigma}_{d-1} = \max\left\{t+1, \left\lceil \frac{r-d+1}{\widehat{m}-d+1} \right\rceil\right\}.$$

The additional bounds follow from Lemma 4 and Corollary 1; subsequent recursion steps remain as in (2) and (3). The counting arguments of Theorem 2 remain valid with these stronger starting values. The iteration gives

$$(m_i, \widehat{m}_i) = (14,17), (14,15), (13,15), (13,12), (11,12), (11,5).$$

In the last step, $\widehat{\sigma}_2(5) = \max\{5, \lceil 25/3 \rceil\} = 9$ and $\widehat{\sigma}_1(5) = \lceil 9 \cdot 26/4 \rceil = 59$. Thus every member would be missed by at least 59 of the 23 points, a contradiction. Hence $\rho_{4,3}(23) \geq 28$, whereas the two counting bounds on their own only give $\rho_{4,3}(23) \geq 20$.

For balanced coverings, the same strengthened iteration shows that an $\mathrm{nc}(n,4,3,n)$ or $\mathrm{nc}(n,3,4,n)$ can exist only for $n \geq 26$, and an $\mathrm{nc}(n,4,4,n)$ only for $n \geq 37$.

### 2.2 The Special Case $s = td + 2$

From Lemma 3 we get $|S_i| \leq t+1$ when $s = td+2$, while a minimal covering has no member of size less than $t$. It therefore consists of $(t+1)$-sets and the $t$-sets that they leave uncovered. For a family $\mathcal{F}$ on a finite set $X$, we write

$$\partial_j \mathcal{F} := \{T \subseteq X : |T| = j,\ T \subseteq F \text{ for some } F \in \mathcal{F}\}$$

for its $j$-shadow. We call $\mathcal{F}$ *intersecting* if any two of its members have a common point. Starting from the covering consisting of all $\binom{s}{t}$ individual $t$-sets, replacing those contained in members of $\mathcal{F}$ by the members of $\mathcal{F}$ themselves reduces the number of members by $|\partial_t \mathcal{F}| - |\mathcal{F}|$. The next proposition characterizes when this gives an NCSC, reducing the determination of $\rho_{t,d}(td+2)$ to an extremal problem for intersecting families.

**Proposition 1.** *Let $t, d \geq 2$ and $s = td+2$. Then*

$$\rho_{t,d}(s) = \binom{s}{t} - \max_{\substack{\mathcal{F} \subseteq \binom{U_s}{t+1} \\ \mathcal{F} \text{ intersecting}}} \big(|\partial_t \mathcal{F}| - |\mathcal{F}|\big). \tag{5}$$

*Every optimal covering consists of a maximizing $\mathcal{F}$ and all $t$-sets outside $\partial_t \mathcal{F}$. In particular,*

$$\binom{s-t-1}{t} \leq \rho_{t,d}(s) \leq \binom{s-1}{t}.$$

*Proof.* If two $(t+1)$-members were disjoint, they would leave $(d-2)t$ points. Partitioning those points into at most $d-2$ sets of size at most $t$, and covering each by a member, would cover $U_s$ with at most $d$ members. Thus the $(t+1)$-members must intersect pairwise.

Conversely, take any intersecting $\mathcal{F}$ and add every uncovered $t$-set. If $d$ selected members include $j \geq 1$ members of $\mathcal{F}$, the first of those covers $t+1$ points and each further one adds at most $t$. Their union therefore has cardinality at most

$$(t+1) + (j-1)t + (d-j)t = td + 1 < s.$$

Finally, for the remaining case $j = 0$, the union has size at most $td$, proving the first formula and the description of the optima. For the lower bound, consider an optimal covering, consisting of an intersecting family $\mathcal{F}$ and all $t$-sets outside $\partial_t\mathcal{F}$. If $\mathcal{F} = \varnothing$, it has $\binom{s}{t} \geq \binom{s-t-1}{t}$ members, so let $F_0 \in \mathcal{F}$. There are $\binom{s-t-1}{t}$ $t$-sets disjoint from $F_0$. Every $F \in \mathcal{F}$ meets $F_0$, so $|F \setminus F_0| \leq t$, and hence $F$ contains at most one of these $t$-sets, namely $F \setminus F_0$. Thus at most $|\mathcal{F}|$ of them lie in $\partial_t\mathcal{F}$, and the remaining at least $\binom{s-t-1}{t} - |\mathcal{F}|$ of them are members of the covering. Together with the $|\mathcal{F}|$ members of size $t+1$, the covering has at least $\binom{s-t-1}{t}$ members.

For the upper bound, fix a point $p$ and let $\mathcal{F}$ consist of all $\binom{s-1}{t}$ $(t+1)$-sets containing $p$. Any two of them share $p$, meaning that $\mathcal{F}$ is intersecting. Moreover, every $t$-set $T$ lies in some member of $\mathcal{F}$, namely in $T \cup \{p\}$ if $p \notin T$, and in $T \cup \{q\}$ for any $q \notin T$ otherwise. Hence $\partial_t\mathcal{F} = \binom{U_s}{t}$, and the covering consists of $\mathcal{F}$ alone, giving $\rho_{t,d}(s) \leq \binom{s-1}{t}$. □

For a family $\mathcal{A}$, its *transversal number* $\tau(\mathcal{A})$ is the minimal size of a set meeting every member of $\mathcal{A}$. Taking complements of the members, an NCSC of degree $t$ and order $d$ corresponds to a family in which every choice of at most $d$ members has a common point and whose transversal number exceeds $t$ [EL75].

When $d = 2$, the individual $t$-sets can be avoided altogether, turning the minimization into a problem in which all members have the same size.

**Proposition 2.** *For $t \geq 1$ and $s = 2t+2$, there exists an optimal covering for which all members have size $t+1$. Hence*

$$\rho_{t,2}(2t+2) = \min\{|\mathcal{A}| : \mathcal{A} \subseteq \tbinom{U_{2t+2}}{t+1} \text{ is intersecting}, \tau(\mathcal{A}) = t+1\}, \qquad (6)$$

*where $\mathcal{A}$ need not cover $U_{2t+2}$, i.e. some points may lie in none of its members.*

*Proof.* Let $k = t+1$. Among all minimal-size coverings, choose one with as many $k$-members as possible. If a $(k-1)$-member $T$ remains, define $Y = U_{2t+2} \setminus T$. Then, at least one $k$-set $Y \setminus \{y\}$ is missing, as otherwise any one of these sets could be deleted, since each of its $(k-1)$-subsets lies in another. Replace $T$ by $T \cup \{y\}$, which preserves coverage. Two members can now cover the $2k$ points only if both have size $k$ and are complements, but the complement of the new member was chosen to be absent. This contradicts the maximal choice of the number of $k$-members.

Complementing such a covering gives an intersecting family $\mathcal{A}$ of $k$-sets. By the coverage condition of NCSCs, we know that no $(k-1)$-set meets every member of $\mathcal{A}$, thus $\tau(\mathcal{A}) \geq k$. Since any member itself meets all the others by the intersecting property, we get equality. Conversely, complementing any family on the right-hand side of (6) gives the required covering. □

## 3 A New Construction of Balanced Coverings

Balanced coverings are of particular interest for practically securing cryptographic implementations in hardware, as the number of input and output shares being equal allows reusing the output shares of one round function as the input shares of the next. This is particularly useful as symmetric ciphers apply the same round function repeatedly. Motivated by their practical relevance, we describe several approaches to finding balanced non-complete set coverings.

Note that whenever a minimal balanced covering $\mathrm{nc}(n,t,d,n)$ was found, we can apply duality to get $\mathrm{nc}(n,d,t,n)$, which will also be the minimal balanced covering for the swapped parameters $d,t$. To see this, if an $\mathrm{nc}(n',d,t,n')$ with $n' < n$ exists, it would dualize to $\mathrm{nc}(n',t,d,n')$, which would contradict the minimality of $\mathrm{nc}(n,t,d,n)$.

### 3.1 $k$-regular Non-Complete Set Coverings

Since a balanced covering has as many members as points, a natural restriction is to require that all members have the same size and that all points have the same degree. Such coverings are considerably easier to search for, as both the member sizes and the degrees are then determined by a single parameter $k$, which in turn is restricted by the counting bounds of Section 2.

**Definition 3.** *For $k \geq 1$, a non-complete set covering $\mathcal{C} = (S_i)_{i \in U_r}$ of $U_s$ is called* $k$-regular *if*

1. *every member $S_i$ has exactly $k$ elements, and*
2. *every point $p \in U_s$ has $\deg(p) = k$.*

*Equivalently, its incidence matrix $X^{(\mathcal{C})}$ has exactly $k$ ones per row and column.*

Counting the incidences of $X^{(\mathcal{C})}$ by columns and by rows gives $kr = \sum_i |S_i| = \sum_p \deg(p) = ks$, so every $k$-regular covering is balanced, i.e. $r = s =: n$. Throughout, we write $\widehat{k} := n - k$. Since the incidence matrix $J - (X^{(\mathcal{C})})^T$ of the dual then has exactly $\widehat{k}$ ones per row and column, the dual of a $k$-regular covering is $\widehat{k}$-regular, justifying this notation.

As a first consequence, the counting bounds of Section 2 immediately restrict the possible values of $k$.

**Lemma 5.** *Let $\sigma_j$ and $\widehat{\sigma}_j$ be defined as in* (2) *and* (3) *with $r = n$, $m = k$ and $\widehat{m} = \widehat{k}$. If a $k$-regular $\mathrm{nc}(n,t,d,n)$ exists, then*

1. $(t-1)d + 1 \leq k \leq n - (d-1)t - 1$,
2. $n\binom{k}{j} \geq \sigma_j \binom{n}{j}$ *for* $1 \leq j \leq t$,
3. $n\binom{\widehat{k}}{j} \geq \widehat{\sigma}_j \binom{n}{j}$ *for* $1 \leq j \leq d$.

*Proof.* Let $\mathcal{C}$ be a $k$-regular $\mathrm{nc}(n,t,d,n)$. By Lemma 3, every point has degree at least $(t-1)d+1$ and every member has at most $n-(d-1)t-1$ elements, and since both quantities equal $k$, this gives the first claim. As all members have at most $k$ elements, Theorem 1 applies with $r=n$ and $m=k$, giving the second claim. Finally, the dual $\widehat{\mathcal{C}}$ is a $\widehat{k}$-regular $\mathrm{nc}(n,d,t,n)$, so the third claim is exactly the second one for $\widehat{\mathcal{C}}$, with the roles of $t$ and $d$ exchanged and $k$ replaced by $\widehat{k}$. □

The second and third conditions rely on the lower bounds $\lambda(T) \geq \sigma_{|T|}$ and $\mu(H) \geq \widehat{\sigma}_{|H|}$, which are obtained purely by counting, starting from the trivial bound $\lambda(T) \geq 1$ for $|T| = t$. However, by Lemma 4 and Corollary 1, every $j$-set $T$ with $j < t$ moreover satisfies $\lambda(T) \geq \rho_{t-j,d}(n-j) \geq (t-j)d+1$, and dually $\mu(H) \geq (d-j)t+1$ for every $j$-set $H$ with $j < d$, which is often larger. Taking the larger of both bounds in every step of the recursion, we define for $t \leq k \leq n-d$

$$\sigma_t^+ := 1, \quad \sigma_j^+ := \max\Big\{(t-j)d+1, \Big\lceil \sigma_{j+1}^+ \frac{n-j}{k-j} \Big\rceil\Big\} \quad (j = t-1,\dots,1), \tag{7}$$

$$\widehat{\sigma}_d^+ := 1, \quad \widehat{\sigma}_j^+ := \max\Big\{(d-j)t+1, \Big\lceil \widehat{\sigma}_{j+1}^+ \frac{n-j}{\widehat{k}-j} \Big\rceil\Big\} \quad (j = d-1,\dots,1). \tag{8}$$

**Lemma 6.** *Let $\mathcal{C}$ be a $k$-regular $\mathrm{nc}(n,t,d,n)$. Then $t \leq k \leq n-d$, and*

$$\lambda(T) \geq \sigma_{|T|}^+ \quad (1 \leq |T| \leq t), \qquad \mu(H) \geq \widehat{\sigma}_{|H|}^+ \quad (1 \leq |H| \leq d).$$

*In particular, $\sigma_1^+ \leq k$ and $\widehat{\sigma}_1^+ \leq \widehat{k}$.*

*Proof.* Every $t$-set is contained in a member of size $k$, so $k \geq t$, and since $\widehat{\mathcal{C}}$ is a $\widehat{k}$-regular $\mathrm{nc}(n,d,t,n)$, the same argument gives $\widehat{k} \geq d$. As $\mu_{\mathcal{C}}(H) = \lambda_{\widehat{\mathcal{C}}}(H)$, it suffices to prove the bounds on $\lambda$, which we do by downward induction on $j = |T|$, starting from $\lambda(T) \geq 1 = \sigma_t^+$ for $|T| = t$. For $|T| = j < t$, we have $\lambda(T) \geq (t-j)d+1$ by Lemma 4 and Corollary 1. Moreover, every member containing $T$ has exactly $k$ elements, so counting the pairs $(x,i)$ with $x \notin T$ and $T \cup \{x\} \subseteq S_i$ gives

$$(k-j)\,\lambda(T) = \sum_{x \in U_n \setminus T} \lambda(T \cup \{x\}) \geq (n-j)\,\sigma_{j+1}^+,$$

and as $k-j > 0$, we obtain $\lambda(T) \geq \sigma_j^+$. Finally, $k$-regularity gives $\lambda(\{x\}) = k$, and thus $\sigma_1^+ \leq k$. □

The conditions $\sigma_1^+ \leq k$ and $\widehat{\sigma}_1^+ \leq \widehat{k}$ of Lemma 6 are at least as strong as the three conditions of Lemma 5, i.e. every $k$ satisfying the former also satisfies the latter. For the first condition, note that $k \geq \sigma_1^+ \geq (t-1)d+1$ and $\widehat{k} \geq \widehat{\sigma}_1^+ \geq (d-1)t+1$, where the latter is equivalent to $k \leq n-(d-1)t-1$.

Moreover, by (7) we have $\sigma_j^+ \leq \sigma_1^+ \prod_{i=1}^{j-1} \frac{k-i}{n-i}$ as well as $\sigma_j^+ \geq \sigma_j$, so $\sigma_1^+ \leq k$ implies $n\binom{k}{j} \geq \sigma_j^+ \binom{n}{j} \geq \sigma_j \binom{n}{j}$ for all $1 \leq j \leq t$, and dually $\widehat{\sigma}_1^+ \leq \widehat{k}$ implies the

third condition. In fact, they are considerably stronger, e.g. for $(t,d) = (4,3)$, $n = 21$ and $k = 12$ we have $\sigma_1 = 8 \leq k$, whereas $\sigma_1^+ = 15 > k$.

Since $\sigma_1^+ \leq k$ and $\widehat{\sigma}_1^+ \leq \widehat{k}$ are necessary for the existence of a $k$-regular $\mathrm{nc}(n,t,d,n)$ by Lemma 6, they yield a lower bound on $n$. We write $\nu_{\mathrm{reg}}(t,d)$ for the smallest $n$ for which some $t \leq k \leq n-d$ satisfies both conditions, which we compute by checking all such $k$ for increasing $n$.

By Lemma 6, every $k$-regular $\mathrm{nc}(n,t,d,n)$ has $n \geq \nu_{\mathrm{reg}}(t,d)$, and since the conditions are exchanged under $(t,d,k) \mapsto (d,t,\widehat{k})$, we have $\nu_{\mathrm{reg}}(t,d) = \nu_{\mathrm{reg}}(d,t)$. For comparison, we write $\nu_{\mathrm{bal}}(t,d) := \min\{n \mid \rho_{t,d}(n) \leq n\}$ for the smallest number of points admitting a balanced covering. We summarize the values of $\nu_{\mathrm{reg}}$ and $\nu_{\mathrm{bal}}$ for various $(t,d)$ in Table 2. Note that, as a balanced covering need not be regular, neither $\nu_{\mathrm{bal}}$ nor $\nu_{\mathrm{reg}}$ bounds the other in general. Nevertheless, in all cases settled so far they coincide, see Table 2.

**Table 2.** Lower bounds $\nu_{\mathrm{reg}}(t,d)$ on the number of points of $k$-regular balanced coverings, compared to the smallest number of points $\nu_{\mathrm{bal}}(t,d)$ of a balanced covering. Intervals give the best known lower and upper bounds on $\nu_{\mathrm{bal}}(t,d)$.

| $(t,d)$ | $(2,2)$ | $(3,2)$ | $(2,3)$ | $(4,2)$ | $(2,4)$ | $(3,3)$ | $(4,3)$ | $(3,4)$ | $(4,4)$ |
|---|---|---|---|---|---|---|---|---|---|
| $\nu_{\mathrm{reg}}$ | 6 | 10 | 10 | 15 | 15 | 18 | 27 | 27 | 46 |
| $\nu_{\mathrm{bal}}$ | 6 | 10 | 10 | 15 | 15 | 18 | $[26,34]$ | $[26,34]$ | $[37,67]$ |

### 3.2 Group Actions and Translate Coverings

A natural way to construct coverings with large amounts of symmetry is to start from a single subset of a group and to take all of its translates under the action of this group. In this subsection, we formalize this construction, characterize the resulting families by their automorphism groups, and translate the conditions of a non-complete covering into conditions on a single subset of the group.

**Definition 4.** *Let $G$ be a finite group of order $n$. For a subset $B \subseteq G$, we define its* translate covering *as the family of its right translates*

$$\mathrm{Cov}_G(B) := (Bg)_{g \in G},$$

*and call $B$ its* base block.

Note that $\mathrm{Cov}_G(B)$ always consists of $n$ members on the $n$ points of $G$, i.e. it is balanced. Moreover, two translates $Bg$ and $Bh$ coincide iff $gh^{-1} \in \mathrm{stab}_G(B) := \{g \in G \mid Bg = B\}$, hence every member occurs exactly $|\mathrm{stab}_G(B)|$ times, and the members are pairwise distinct iff $\mathrm{stab}_G(B) = 1$. Furthermore, every translate covering is regular, with $k$ given by the size of its base block.

**Lemma 7.** *Let $G$ be a finite group of order $n$ and $B \subseteq G$. Then $\mathrm{Cov}_G(B) = (Bg)_{g \in G}$ is $|B|$-regular.*

*Proof.* Right multiplication by $g$ is a bijection of $G$, so $|Bg| = |B|$ for every $g \in G$. For $x \in G$ we have $x \in Bg$ iff $xg^{-1} \in B$ iff $g \in B^{-1}x$. Hence $x$ lies in exactly $|\{g \mid x \in Bg\}| = |B^{-1}x| = |B|$ members, since inversion and right multiplication by $x$ are bijections. □

The group $G$ acts on itself by right multiplication, and this action maps the translate $Bg$ to $Bgh$. Therefore, $G$ is contained in the automorphism group of $\mathrm{Cov}_G(B)$, where an automorphism of a family $(S_i)_{i\in U_r}$ of subsets of $U_s$ is a permutation $\pi$ of $U_s$ such that every set $\pi(S_i)$ occurs in the family as often as $S_i$. Similarly, two families are isomorphic if a bijection between their point sets maps the members of one onto the members of the other, counted with multiplicity. Conversely, a suitable subgroup of the automorphism group identifies a family with a translate covering.

**Theorem 3.** *A family $\mathcal{C}$ of $n$ subsets of $U_n$ is isomorphic to a translate covering over $G$ iff $\mathrm{Aut}(\mathcal{C})$ contains a subgroup isomorphic to $G$ which acts regularly on $U_n$ and transitively on the members of $\mathcal{C}$.*

*Proof.* Let $\mathcal{C} = \mathrm{Cov}_G(B)$, and for $h \in G$ let $\pi_h(x) = xh^{-1}$. Then $\pi_h(Bg) = B(gh^{-1})$, and as $g \mapsto gh^{-1}$ is a bijection of $G$, every $\pi_h$ permutes the members of $\mathcal{C}$ including their multiplicities, i.e. $\pi_h \in \mathrm{Aut}(\mathcal{C})$. Moreover, $\pi_h\pi_{h'} = \pi_{hh'}$ and $\pi_h = \mathrm{id}$ only for $h = e$, so $h \mapsto \pi_h$ embeds $G$ into $\mathrm{Aut}(\mathcal{C})$. Its image acts regularly on $G$, as for $x, y \in G$ exactly $h = y^{-1}x$ satisfies $\pi_h(x) = y$, and transitively on the members, as $\pi_{g^{-1}}(B) = Bg$.

Conversely, let $\mathcal{C} = (S_i)_{i\in U_n}$, and let $K \leq \mathrm{Aut}(\mathcal{C})$ be a subgroup with the stated properties, where $h \mapsto \pi_h$ is an isomorphism $G \xrightarrow{\sim} K$. Fix a point $p_0 \in U_n$ and define $\varphi\colon G \to U_n$ by $\varphi(g) = \pi_{g^{-1}}(p_0)$. As $K$ acts regularly on $U_n$, the map $\varphi$ is a bijection, and

$$\pi_h(\varphi(g)) = \pi_{hg^{-1}}(p_0) = \varphi(gh^{-1}),$$

i.e. under $\varphi$, the permutation $\pi_h$ becomes right multiplication by $h^{-1}$. Fix an index $i_0 \in U_n$ and let $B = \varphi^{-1}(S_{i_0}) \subseteq G$. Since $K$ acts transitively on the members, the distinct members of $\mathcal{C}$ are exactly the sets $\pi_h(S_{i_0}) = \varphi(Bh^{-1})$ for $h \in G$, i.e. the images of the right translates of $B$, of which there are $n/|\mathrm{stab}_G(B)|$ by the orbit–stabilizer theorem. As every $\pi_h$ preserves multiplicities and $K$ acts transitively, all distinct members of $\mathcal{C}$ occur equally often, namely $|\mathrm{stab}_G(B)|$ times, as there are $n$ members in total. This is also the multiplicity of every member of $\mathrm{Cov}_G(B)$, as $Bg = Bg'$ iff $g'g^{-1} \in \mathrm{stab}_G(B)$. Hence $\varphi$ maps the members of $\mathrm{Cov}_G(B)$ bijectively, including multiplicities, onto those of $\mathcal{C}$, and the two families are isomorphic. □

Moreover, by Lagrange's theorem, the order of such a subgroup divides $|\mathrm{Aut}(\mathcal{C})|$, leading to the following corollary ruling out the existence of a translate covering for specific families of subsets.

**Corollary 4.** *A family $\mathcal{C}$ of $n$ subsets of $U_n$ cannot be isomorphic to a translate covering if $|\mathrm{Aut}(\mathcal{C})|$ is not divisible by $n$.*

Since the automorphism group of a family can be computed efficiently in practice, this gives a quick test for a given covering. However, the converse does not hold in general, as a subgroup of order $n$ does not necessarily act regularly on the points.

Next, we formulate conditions on translate coverings in order to be non-complete set coverings. For that, we call a family of subsets of $U_s$ a *$t$-cover* if every $t$-subset of $U_s$ is contained in one of its members.

**Lemma 8.** *A family $\mathcal{C}$ of $r$ subsets of $U_s$ is an $\mathrm{nc}(s,t,d,r)$ iff $\mathcal{C}$ is a $t$-cover and $\widehat{\mathcal{C}}$ is a $d$-cover, when $r \geq d$. Moreover, for a finite group $G$ and $B \subseteq G$, the dual of $\mathrm{Cov}_G(B)$ is $\mathrm{Cov}_G(\overline{B}^{-1})$, where $\overline{B} = G \setminus B$. In particular, $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n,t,d,n)$ iff $\mathrm{Cov}_G(B)$ is a $t$-cover and $\mathrm{Cov}_G(\overline{B}^{-1})$ is a $d$-cover.*

*Proof.* For $H \subseteq U_r$ we have $H \subseteq R_p$ iff $p \notin S_i$ for all $i \in H$, i.e. the members indexed by $H$ miss a common point iff $H$ is contained in a member of $\widehat{\mathcal{C}}$, which proves the first statement. For $\mathrm{Cov}_G(B)$ indexed by $g \in G$ and $x \in G$, we have

$$R_x = \{g \in G : x \notin Bg\} = \{g \in G : xg^{-1} \in \overline{B}\} = \overline{B}^{-1}x,$$

so the dual is $(\overline{B}^{-1}x)_{x\in G} = \mathrm{Cov}_G(\overline{B}^{-1})$, and the last statement follows from the first. □

Thus both conditions only depend on the base block $B$, and the search for a balanced covering on $n$ points reduces to the search for a single subset of a group of order $n$.

Finally, by Lemma 7, every translate covering $\mathrm{Cov}_G(B)$ is $|B|$-regular, so the bound $\nu_{\mathrm{reg}}$ from Lemma 6 applies to it. The converse does not hold, as e.g. $\mathrm{nc}(18,3,3,18)$ is 9-regular but not a translate covering. For $(2,2)$, $(3,2)$ and $(2,3)$ the bound $\nu_{\mathrm{reg}}$ is attained by the cyclic coverings below. For $(4,2)$ and $(3,3)$ it coincides with the threshold of [FFL26], i.e. $\nu_{\mathrm{reg}} = 15$ resp. $\nu_{\mathrm{reg}} = 18$. Only for $(4,3)$, $(3,4)$ and $(4,4)$ does Lemma 6 improve on the general bounds, to $\nu_{\mathrm{reg}} = 27$ resp. $\nu_{\mathrm{reg}} = 46$. Moreover, for $(4,3)$ and $(3,4)$ the case $n = 28$ can be skipped, since no $k$ satisfies Lemma 5 there.

Beyond giving a starting point for the search, Lemma 5 also restricts the possible sizes $k = |B|$ of a base block. Still, for a fixed group $G$ of order $n$ and an admissible $k$, a naive search has to test $\binom{n}{k}$ candidates against the two conditions of Lemma 8, which is infeasible already for slightly larger $n$. The algorithm of the next subsection reduces this search space considerably.

In terms of the base block, the quantities $\lambda$ and $\mu$ of a translate covering are intersections of translates. Let $G$ be a group of order $n$, let $B \subseteq G$ with $|B| = k$, and index the members of $\mathrm{Cov}_G(B)$ by $g \in G$. Then $x \in Bg$ iff $g \in B^{-1}x$, and $G \setminus Bg = \overline{B}g$, so

$$\lambda(T) = \Big|\bigcap_{x\in T} B^{-1}x\Big|, \qquad \mu(H) = \Big|\bigcap_{g\in H} \overline{B}g\Big| \tag{9}$$

for every set $T \subseteq G$ of points and every set $H \subseteq G$ of member labels. In particular, $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n,t,d,n)$ iff all intersections of $t$ translates of $B^{-1}$ and all intersections of $d$ translates of $\overline{B}$ are nonempty, in accordance with Lemma 8. Moreover, as $\mathrm{Cov}_G(B)$ is $k$-regular by Lemma 7, Lemma 6 bounds all intersections of fewer translates from below by $\sigma_j^+$ and $\widehat{\sigma}_j^+$, respectively.

These bounds can optionally be refined by taking the action of $G$ on its subsets into account. For $1 \le j \le n$, the group $G$ acts on its $j$-subsets by right multiplication, and we denote the set of orbits by $\mathcal{O}_j(G)$. Since sets in the same orbit have conjugate stabilizers, all of them have the same stabilizer order, and we let $a_{j,h}$ denote the number of orbits in $\mathcal{O}_j(G)$ with stabilizer order $h$. These numbers only depend on $G$ and $j$, so they can be reused for all sizes $k$.

**Lemma 9.** *Let $G$ be a group of order $n$ and $B \subseteq G$ with $|B| = k$ such that $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n,t,d,n)$. Then*

$$\binom{k}{j} \ge \sum_{h=1}^{n} a_{j,h} \left\lceil \sigma_j^+ / h \right\rceil \quad (1 \le j \le t), \qquad \binom{n-k}{j} \ge \sum_{h=1}^{n} a_{j,h} \left\lceil \widehat{\sigma}_j^+ / h \right\rceil \quad (1 \le j \le d). \tag{10}$$

*Proof.* Fix $1 \le j \le t$ and an orbit $\mathcal{O} \in \mathcal{O}_j(G)$ with stabilizer order $h$, so that $|\mathcal{O}| = n/h$. By (9), we have $\lambda(Tg) = |(\bigcap_{x \in T} B^{-1}x)g| = \lambda(T)$, so $\lambda$ takes a constant value $\lambda_{\mathcal{O}}$ on $\mathcal{O}$, and $\lambda_{\mathcal{O}} \ge \sigma_j^+$ by Lemmas 6 and 7. Let $\kappa_{\mathcal{O}}$ be the number of sets in $\mathcal{O}$ that are contained in $B$. Since $T \subseteq Bg$ iff $Tg^{-1} \subseteq B$, where $Tg^{-1} \in \mathcal{O}$, counting the pairs $(T,g)$ with $T \in \mathcal{O}$ and $T \subseteq Bg$ in two ways gives

$$n\,\kappa_{\mathcal{O}} = |\mathcal{O}|\,\lambda_{\mathcal{O}} = (n/h)\,\lambda_{\mathcal{O}},$$

i.e. $\kappa_{\mathcal{O}} = \lambda_{\mathcal{O}}/h \ge \sigma_j^+/h$, and as $\kappa_{\mathcal{O}}$ is an integer, we obtain $\kappa_{\mathcal{O}} \ge \left\lceil \sigma_j^+/h \right\rceil$. Since every $j$-subset of $B$ lies in exactly one orbit, summing over all orbits gives the first inequality. The second one follows by applying the first to the dual $\mathrm{Cov}_G(\overline{B}^{-1})$, which is an $(n-k)$-regular $\mathrm{nc}(n,d,t,n)$ by Lemma 8. □

Note that $\sum_h a_{j,h}\, n/h = \binom{n}{j}$, so without taking ceilings, the right-hand side of (10) equals $\sigma_j^+ \binom{n}{j}/n$, which is already bounded by $\binom{k}{j}$ whenever $\sigma_1^+ \le k$. Hence (10) improves on Lemma 6 only through orbits with non-trivial stabilizers.

### 3.3 Algorithm for Finding Translate Coverings

We now give an algorithm that searches for translate coverings over a given list of groups of fixed order. Its input consists of integers $2 \le t, d \le n$ and a finite ordered list $\mathcal{G}$ of groups of order $n$, and it either returns a group $G \in \mathcal{G}$ together with a base block $B \subseteq G$ such that $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n,t,d,n)$, or reports that no such pair exists. Here, we restrict the search to base blocks with $\mathrm{stab}_G(B) = 1$, i.e. to coverings whose $n$ members are pairwise distinct. For an exhaustive search over all groups of order $n$, we take one representative of each isomorphism class, e.g. `SmallGroup(n,i)` for $1 \le i \le$ `NumberSmallGroups(n)`

from GAP's Small Groups Library.[2] While its running time is exponential in $n$, the algorithm is nevertheless a useful tool to find new translate coverings in practice. The algorithm is given in Algorithm 1, where we fix an ordering $G = \{g_0, \dots, g_{n-1}\}$ with $g_0 = e$ for each group $G \in \mathcal{G}$.

Compared to testing all subsets of $G$, the algorithm reduces the search space in three ways. First, it only considers sizes $k$ admitted by Lemma 6, and for a fixed group $G$ optionally also by Lemma 9. Second, it uses duality to fix $d$ elements $D = \{g_0, \dots, g_{d-1}\}$ of the complement $\overline{B}$, so that only $\binom{n-d}{\widehat{k}-d}$ candidates remain for each pair $(G, k)$. Third, it tests each candidate by computing intersections of translates of $\overline{B}$ and of $B^{-1}$ incrementally, and rejects it as soon as one of these intersections is smaller than the corresponding bound $\widehat{\sigma}_j^+$ resp. $\sigma_j^+$. As these bounds are large for intersections of only few translates, most candidates are already rejected by the pairwise intersections in the first test, and only few of them reach the subroutine Cover. Conversely, Cover skips the enumeration entirely whenever a simple union bound already guarantees that all intersections are nonempty.

**Theorem 4.** *Let $2 \le t, d \le n$ be integers and let $\mathcal{G}$ be a finite ordered list of groups of order $n$. Then Algorithm 1 terminates, and it returns* `found` *iff some $G \in \mathcal{G}$ has a subset $B$ with $\mathrm{stab}_G(B) = 1$ such that $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n, t, d, n)$. Moreover, termination is guaranteed within checking at most*

$$|\mathcal{G}| \sum_{k=t}^{n-d} \binom{n-d}{n-k-d} \le |\mathcal{G}|\, 2^{n-d}$$

*candidates. In particular, if $\mathcal{G}$ contains every isomorphism type of order $n$, then* `excluded` *proves that no $\mathrm{nc}(n, t, d, n)$ with pairwise distinct members arises as a translate covering.*

*Proof.* For each pair $(G, k)$, the algorithm enumerates the $\binom{n-d}{\widehat{k}-d}$ sets $E$, and each subsequent test considers only finitely many intersections, so the algorithm terminates. Summing over all groups and sizes gives the stated number of candidates, and the binomial theorem gives the final inequality.

We first justify the restrictions in the intersection tests. For $Q \subseteq G$, a nonempty set $A \subseteq G$ and $a_0 \in A$, right multiplication by $a_0^{-1}$ gives

$$\Big|\bigcap_{a \in A} Qa\Big| = \Big|\bigcap_{a \in A} Q(aa_0^{-1})\Big|,$$

so we may assume $e \in A$, and the intersections of $c$ translates of $Q$ are determined by the index sequences $1 \le i_1 < \cdots < i_{c-1} \le n-1$ enumerated in Cover. For $c = 2$, we moreover have $|Q \cap Qg| = |Q \cap Qg^{-1}|$, and $Qg = Q$ iff $Qg^{-1} = Q$, so in the first test, as well as for the distinctness of the translates, it suffices to

[2] See *The Small Groups Library*, Chapter 1, https://gap-packages.github.io/smallgrp/doc/chap1.html.

**Algorithm 1** Search for translate coverings

**Require:** $n, t, d$ and a list $\mathcal{G}$ of groups $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$ of order $n$
**Ensure:** `found` with $(G, B)$, or `excluded`

$\mathcal{K} \leftarrow \{k \in \{t, \ldots, n-d\} : \sigma_1^+ \le k \text{ and } \widehat{\sigma}_1^+ \le n-k\}$ ▷ $\sigma_j^+, \widehat{\sigma}_j^+$ from (7), (8)
**if** $\mathcal{K} = \emptyset$ **then**
  **return** `excluded`
**end if**
**for all** $G \in \mathcal{G}$ **do**
  optionally compute $a_{j,h}$ for some $j \le \max\{t, d\}$
  **for all** $k \in \mathcal{K}$ satisfying (10) **do**
    $\widehat{k} \leftarrow n-k, \quad D \leftarrow \{g_0, \ldots, g_{d-1}\}$
    $P \leftarrow$ one element from each $\{g, g^{-1}\}$, $g \ne e$
    **for all** $E \subseteq G \setminus D$ with $|E| = \widehat{k} - d$ **do**
      $B \leftarrow G \setminus (D \cup E)$
      **if** some $g \in P$ has $Bg = B$, $|\overline{B} \cap \overline{B}g| < \widehat{\sigma}_2^+$ or $|B^{-1} \cap B^{-1}g| < \sigma_2^+$ **then**
        **continue**
      **end if**
      **if** $\textsc{Cover}(\overline{B}, d, \widehat{\sigma}^+)$ **and** $\textsc{Cover}(B^{-1}, t, \sigma^+)$ **then**
        **return** `found`, $(G, B)$
      **end if**
    **end for**
  **end for**
**end for**
**return** `excluded`

**function** $\textsc{Cover}(Q, c, \Theta)$
  **if** $c = 2$ **or** $n - c(n - |Q|) > 0$ **then**
    **return** `true`
  **end if**
  **for all** $1 \le i_1 < \cdots < i_{c-1} \le n-1$ **do**
    $I_1 \leftarrow Q$
    **for** $j = 1, \ldots, c-1$ **do**
      $I_{j+1} \leftarrow I_j \cap Qg_{i_j}$
      **if** $j \ge 2$ **and** $|I_{j+1}| < \Theta_{j+1}$ **then**
        **return** `false`
      **end if**
    **end for**
  **end for**
  **return** `true`
**end function**

consider $g \in P$. Finally, for any $g_1, \ldots, g_c \in G$ we have

$$\Big|\bigcap_{a=1}^{c} Qg_a\Big| = n - \Big|\bigcup_{a=1}^{c} (G \setminus Qg_a)\Big| \geq n - c(n - |Q|),$$

so if the right-hand side is positive, all intersections of $c$ translates of $Q$ are nonempty, which justifies the early return in Cover.

Now suppose that the algorithm returns $(G, B)$. Then $Bg \neq B$ for all $g \in P$, and hence for all $g \neq e$, so that $\mathrm{stab}_G(B) = 1$. Moreover, all intersections of $d$ translates of $\overline{B}$ are nonempty: for $d = 2$, this is guaranteed by the first test, as $\widehat{\sigma}_2^+ = 1$, and for $d \geq 3$ it is either guaranteed by the union bound or checked directly in Cover, whose final test requires $|I_d| \geq \widehat{\sigma}_d^+ = 1$. By the same argument, all intersections of $t$ translates of $B^{-1}$ are nonempty, and thus $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n, t, d, n)$ by (9).

Conversely, suppose that some $G \in \mathcal{G}$ has a subset $B$ with $\mathrm{stab}_G(B) = 1$ such that $\mathrm{Cov}_G(B)$ is an $\mathrm{nc}(n, t, d, n)$. By Lemma 8, the dual $\mathrm{Cov}_G(\overline{B}^{-1})$ covers the $d$-set $D^{-1}$, i.e. $D^{-1} \subseteq \overline{B}^{-1}x$ for some $x \in G$, or equivalently $D \subseteq x^{-1}\overline{B}$. Since left multiplication by $x^{-1}$ is a bijection of $G$ with $x^{-1}(Bg) = (x^{-1}B)g$, the covering $\mathrm{Cov}_G(x^{-1}B)$ is isomorphic to $\mathrm{Cov}_G(B)$, and $\mathrm{stab}_G(x^{-1}B) = \mathrm{stab}_G(B) = 1$. Hence we may assume $D \subseteq \overline{B}$, so that $B$ is one of the candidates enumerated for its size $k$. By Lemmas 6 and 9, the size $k$ is not discarded, and by (9), every intersection of $j$ translates of $B^{-1}$ resp. $\overline{B}$ has at least $\sigma_j^+$ resp. $\widehat{\sigma}_j^+$ elements. Thus $B$ passes all tests, and the algorithm returns `found` at the latest when reaching this candidate. Finally, group isomorphisms preserve right translates as well as the defining conditions of a non-complete covering, which proves the last statement. □

In our implementation, the groups are processed in their input order and the sizes $k$ in increasing order. The sets $E$ and the index sequences in Cover are enumerated in lexicographic order of their increasing index lists, so that the intersections determined by unchanged initial indices can be reused when moving to the next sequence. Moreover, Cover is called first for the smaller value of $c$, using $\overline{B}$ first if $t = d$, since this test is cheaper and more likely to reject the candidate. To compute the numbers $a_{j,h}$, we enumerate the $j$-subsets containing $e$ together with their right translates, identify each orbit by the lexicographically least index list among its members, and count the translations fixing it. This suffices since every orbit contains a set containing $e$, as $Aa^{-1}$ contains $e$ for every $a \in A$.

## 4 Explicit Nonexistence Arguments

The bounds of Section 2 apply to all parameters simultaneously, as they only rely on counting, duality and the link structure of a covering. Together with the coverings found in Section 5, they already determine $\rho_{t,d}(s)$ in several cases, but in general, a gap between the lower and upper bounds remains, as evident

from Figure 1. In this section, we close some of these gaps by arguments tailored to specific parameters, combining sharper nonexistence arguments with matching constructions. These range from short combinations of duality and monotonicity, which transfer known values from one parameter set to another, to a structural analysis of the boundary case $s = td+2$, where minimal coverings can be described in terms of intersecting families. In particular, by doing so, we are able to determine $\rho_{3,2}$ and $\rho_{2,3}$ for all parameters $s$, as well as $\rho_{4,2}(s)$ for all $s \geq 26$.

**Proposition 3.** $\rho_{3,3}(19) = 18$.

*Proof.* The covering $\mathrm{nc}(18, 3, 3, 18)$ from Section 5 together with Lemma 2 gives an $\mathrm{nc}(19, 3, 3, 18)$, so $\rho_{3,3}(19) \leq 18$. Conversely, suppose that an $\mathrm{nc}(19, 3, 3, r)$ with $r \leq 17$ exists. By Lemma 1, there is an $\mathrm{nc}(r, 3, 3, 19)$, and since $r \leq 17$, Lemma 2 yields an $\mathrm{nc}(17, 3, 3, 19)$. Hence $\rho_{3,3}(17) \leq 19$, contradicting $\rho_{3,3}(17) \geq 20$ from [FFL26, Table 3]. □

**Theorem 5.** *There is no* $\mathrm{nc}(8, 3, 2, r)$ *with* $r \leq 16$. *Consequently,* $\rho_{3,2}(8) = 17$.

*Proof.* Suppose that such a covering exists. By Proposition 2, there then exists a family $\mathcal{C}$ of $r \leq 16$ 4-subsets of $U_8$ which contains every 3-subset of $U_8$ in some member, and no two complementary members. Applying Definition 2 with $m = 4$ gives $\deg(x) \geq 7$ for every $x$.

*Case 1:* $\deg(x) = 7$ *for some* $x$. Let $Y = U_8 \setminus \{x\}$. The seven sets $S \setminus \{x\}$ with $x \in S$ are triples covering the 21 pairs of $Y$, so they cover every pair exactly once, i.e. they are the lines of the Fano plane on $Y$. Since any two lines meet, the 28 sets consisting of a line and a further point are distinct, and the remaining seven 4-subsets of $Y$ are the complements of lines. These are not members, as the complement of a line $\ell$ in $Y$ is complementary to the member $\{x\} \cup \ell$. Hence every member contained in $Y$ contains exactly one line, and thus exactly three of the 28 triples of $Y$ that are not lines. These 28 triples lie in no member through $x$, so they must be covered by the at most $r - 7 \leq 9$ members contained in $Y$, which contain at most 27 of them, a contradiction.

*Case 2:* $\deg(x) \geq 8$ *for all* $x$. Then $64 \leq \sum_x \deg(x) = \sum_S |S| \leq 4r \leq 64$, so $r = 16$, all members have cardinality 4, and all points have degree 8. For any fixed $x$, the eight triples $S \setminus \{x\}$ contain 24 pairs of $U_8 \setminus \{x\}$, cover all 21 of them, and every point lies in an even number of these pairs. Hence the pairs covered more than once form a graph with three edges and even degrees, i.e. a triangle $\{a, b, c\}$, so $\lambda(\{x, a, b\}) = \lambda(\{x, a, c\}) = \lambda(\{x, b, c\}) = 2$, while $\lambda(T) = 1$ for all other triples $T \ni x$. Applying the same argument to $a$, the triples through $a$ with $\lambda = 2$ form a triangle containing $\{x, b\}$ and $\{x, c\}$, hence also $\{b, c\}$. Thus $Q = \{x, a, b, c\}$ is the unique 4-set containing $x$ all of whose triples $T$ satisfy $\lambda(T) = 2$, and the same argument for a point outside $Q$ gives the same for $Q' = U_8 \setminus Q$.

We show $Q \in \mathcal{C}$. The four triples of $Q$ lie in 8 members in total, counted with multiplicity. The member $Q$ would account for 4 of them, and every other member contributing has the form $T \cup \{y\}$ with $y \in Q'$. For each $y \in Q'$ there is

at most one such member, since two of them would intersect in a triple through $y$ with $\lambda = 2$ that meets $Q$. Hence the members other than $Q$ account for at most 4, so $Q \in \mathcal{C}$, and by symmetry $Q' \in \mathcal{C}$, contradicting non-completeness.

Finally, an explicit $\mathrm{nc}(8, 3, 2, 17)$ is given in [FFL26], giving $\rho_{3,2}(8) = 17$. $\square$

We now determine $\rho_{2,d}(2d+2)$ exactly for all $d \geq 3$. By Proposition 1 with $t = 2$, an optimal $\mathrm{nc}(2d+2, 2, d, r)$ consists of an intersecting family $\mathcal{F}$ of triples together with all pairs not covered by $\mathcal{F}$. Each triple covers three pairs at the cost of a single member, so we have to maximize the saving $|\partial_2\mathcal{F}| - |\mathcal{F}|$ over all intersecting families of triples. Two constructions naturally suggest themselves.

The first one is the *Fano plane* $\mathcal{P}$, i.e. the 7 lines of the projective plane of order two, which we write as the triples

$$123, \quad 145, \quad 167, \quad 246, \quad 257, \quad 347, \quad 356$$

on the points $1, \ldots, 7$. Any two of its triples meet in exactly one point, so $\mathcal{P}$ is intersecting, and every pair of points lies in exactly one triple, so its 7 triples cover all 21 pairs and save 14 members, independently of $s$. The second one grows with $s$. For distinct points $x, y, a, b, c, e \in U_s$, let $W$ consist of the remaining $s-6$ points, and let $\mathcal{D}$ consist of the $s-2$ triples

$$xab, \quad xce, \quad yac, \quad ybe, \qquad xyw \quad (w \in W).$$

Any two of the first four triples meet, and all other triples contain both $x$ and $y$, so $\mathcal{D}$ is intersecting. It covers all $2(s-2)+1$ pairs containing $x$ or $y$, as well as the four pairs $ab, ce, ac, be$, and thus saves $2(s-2)+1+4-(s-2) = s+3$ members. The following theorem shows that these constructions are optimal.

**Theorem 6.** *For $d \geq 3$ and $s = 2d+2$, we have*

$$\rho_{2,d}(s) = \binom{s}{2} - \max\{14, s+3\} = \begin{cases} 14, & d = 3, \\ 31, & d = 4, \\ 2d^2 + d - 4, & d \geq 5. \end{cases}$$

*Moreover, for $d = 3, 4$, the unique optimal covering up to isomorphism consists of $\mathcal{P}$ and all pairs not contained in its triples. For $d \geq 5$, there are exactly three optimal coverings up to isomorphism, consisting of $\mathcal{D}$, $\mathcal{D} \cup \{xae\}$ or $\mathcal{D} \cup \{xae, xbc\}$, together with all pairs not contained in their triples.*

*Proof.* By the discussion above, it suffices to show that every intersecting family $\mathcal{F}$ of triples of $U_s$ satisfies

$$|\partial_2\mathcal{F}| - |\mathcal{F}| \leq \max\{14, s+3\}, \tag{11}$$

since $\mathcal{P}$ and $\mathcal{D}$ attain this bound for $s \leq 10$ and $s \geq 12$, respectively. The values for $d \geq 5$ then follow from $\binom{2d+2}{2} - (2d+5) = 2d^2 + d - 4$.

For $\mathcal{F} = \emptyset$, (11) is trivial. Otherwise, any member of $\mathcal{F}$ meets all others, implying $1 \leq \tau(\mathcal{F}) \leq 3$. Below we distinguish these three cases.

1. $\tau(\mathcal{F}) = 1$. Let $x$ be a point contained in every member. Then every member $\{x, u, v\}$ contains exactly one pair avoiding $x$, namely $\{u, v\}$, and at most $s - 1$ pairs of $\partial_2\mathcal{F}$ contain $x$, so $|\partial_2\mathcal{F}| - |\mathcal{F}| \leq s - 1$.
2. $\tau(\mathcal{F}) = 2$. Let $\{x, y\}$ meet every member, and let $Y = U_s \setminus \{x, y\}$. Then $\mathcal{F}$ decomposes uniquely as

$$\mathcal{F} = \big\{\{x\} \cup p \;\big|\; p \in A\big\} \cup \big\{\{y\} \cup q \;\big|\; q \in B\big\} \cup \big\{\{x, y, z\} \;\big|\; z \in Z\big\}$$

with sets $A, B$ of pairs in $Y$ and $Z \subseteq Y$. Here $A$ and $B$ are nonempty, as otherwise a single point would meet every member, and $p \cap q \neq \emptyset$ for all $p \in A$ and $q \in B$, as $\mathcal{F}$ is intersecting. Let $V_A = \bigcup_{p\in A} p$ and $V_B = \bigcup_{q\in B} q$ be the sets of points covered by $A$ and $B$, respectively. Counting the pairs of $\partial_2\mathcal{F}$ according to whether they contain only $x$, only $y$, both or neither gives

$$\begin{aligned} |\partial_2\mathcal{F}| - |\mathcal{F}| &= |V_A \cup Z| + |V_B \cup Z| + \mathbf{1}_{Z\neq\emptyset} + |A \cup B| - |A| - |B| - |Z| \\ &= |V_A \cup Z| + |V_B \cup Z| - |Z| - |A \cap B| + \mathbf{1}_{Z\neq\emptyset} \qquad (12) \\ &\leq s - 1 + |V_A \cap V_B| - |A \cap B|, \qquad (13) \end{aligned}$$

where the inequality follows from $|V_A \cup Z| + |V_B \cup Z| \leq |V_A \cup V_B \cup Z| + |V_A \cap V_B| + |Z|$, $|V_A \cup V_B \cup Z| \leq s - 2$ and $\mathbf{1}_{Z\neq\emptyset} \leq 1$. It remains to show that $|V_A \cap V_B| - |A \cap B| \leq 4$. If $A$ contains two disjoint pairs, every pair of $B$ meets both of them, so $V_B$ lies in their union and $|V_B| \leq 4$. Otherwise, the pairs of $A$ either lie in a set of three points, so $|V_A| \leq 3$, or they all contain a common point $a$. In the latter case, if some $q \in B$ avoids $a$, then every pair of $A$ is of the form $\{a, z\}$ with $z \in q$, so again $|V_A| \leq 3$. If instead every pair of $B$ contains $a$, then a point $z \neq a$ lies in $V_A \cap V_B$ iff $\{a, z\} \in A \cap B$, so $|V_A \cap V_B| - |A \cap B| = 1$. Hence $|\partial_2\mathcal{F}| - |\mathcal{F}| \leq s + 3$.
3. $\tau(\mathcal{F}) = 3$. Extend $\mathcal{F}$ to an intersecting family of triples that is maximal with respect to inclusion. Adding members cannot decrease $\tau$, so the extension still satisfies $\tau = 3$, and by [PR17, Theorem 1.7], the union of its members, and hence that of $\mathcal{F}$, consists of at most 7 points. Thus $|\partial_2\mathcal{F}| \leq \min\{3|\mathcal{F}|, 21\}$, and

$$|\partial_2\mathcal{F}| - |\mathcal{F}| \leq \min\{2|\mathcal{F}|,\ 21 - |\mathcal{F}|\} \leq 14.$$

It remains to classify the families attaining equality in (11). For $d = 3, 4$, i.e. $s = 8, 10$, the first two cases give at most $s + 3 < 14$, so every optimal family satisfies $\tau(\mathcal{F}) = 3$. Equality then forces $|\mathcal{F}| = 7$ and $|\partial_2\mathcal{F}| = 21$, i.e. the 7 triples lie on 7 points and cover every pair of them exactly once. In particular, every point lies in exactly three triples, which we may label 123, 145 and 167 for the point 1. After relabelling within $\{4, 5\}$ and $\{6, 7\}$, the triple containing 24 is 246, and the pairs 25, 34 and 35 force the triples 257, 347 and 356, so $\mathcal{F} = \mathcal{P}$.

For $d \geq 5$, i.e. $s \geq 12$, we have $s + 3 > 14$, so every optimal family satisfies $\tau(\mathcal{F}) = 2$, with equality in (13) and $|V_A \cap V_B| - |A \cap B| = 4$. As the other cases of this bound give at most 3, $A$ contains two disjoint pairs $p_1, p_2$, and with $Q = p_1 \cup p_2$ we obtain $V_B = Q$, $V_A \cap V_B = Q$ and $A \cap B = \emptyset$. In particular, every pair of $B$ has one point in $p_1$ and one in $p_2$, and as these pairs cover $Q$,

two of them are disjoint. Exchanging the roles of $A$ and $B$ thus gives $V_A = Q$, and we may label $Q = \{a, b, c, e\}$ such that $ab, ce \in A$ and $ac, be \in B$. The only other pairs on $Q$ meeting all pairs of the respective other set are $ae$ and $bc$. Since they are disjoint, they cannot lie in different sets among $A$ and $B$, and since $A \cap B = \emptyset$, neither of them lies in both. Up to exchanging $x$ and $y$ and relabelling, we may thus add none of them, $ae$ to $A$, or both to $A$. Finally, for $V_A = V_B = Q$, the value (12) equals $8 + |Z \setminus Q| - |Z \cap Q| + \mathbf{1}_{Z \neq \emptyset}$, which equals $s+3$ iff $Z = U_s \setminus (\{x, y\} \cup Q) = W$. These are exactly the families $\mathcal{D}$, $\mathcal{D} \cup \{xae\}$ and $\mathcal{D} \cup \{xae, xbc\}$, which are pairwise non-isomorphic, as they have $s-2$, $s-1$ and $s$ members, and by Proposition 1 they yield exactly the optimal coverings of the theorem. □

By duality, Theorem 6 determines how many points a covering of degree $d$ and order two with $2d+2$ members needs, which yields exact values of $\rho_{d,2}(s)$ on entire intervals of $s$.

**Corollary 5.** *For $d \geq 3$, let $s_d^- = \binom{2d+2}{2} - \max\{14, 2d+5\}$ and $s_d^+ = \binom{2d+1}{2}$. Then $\rho_{d,2}(s) = 2d+2$ for $s_d^- \leq s < s_d^+$, and $\rho_{d,2}(s) \geq 2d+3$ for $2d+1 \leq s < s_d^-$.*

*Proof.* By Lemma 1, an $\mathrm{nc}(s, d, 2, 2d+2)$ exists iff an $\mathrm{nc}(2d+2, 2, d, s)$ exists, i.e. iff $s \geq \rho_{2,d}(2d+2) = s_d^-$ by Theorem 6. Moreover, by Corollary 1, an $\mathrm{nc}(s, d, 2, 2d+1)$ exists iff $s \geq s_d^+$, and no covering with fewer members exists. □

For $d = 4$, we have $s_4^- = 31$ and $s_4^+ = 36$, so together with the $\mathrm{nc}(26, 4, 2, 11)$ found in Section 5, we obtain

$$\rho_{4,2}(s) = \begin{cases} 11, & 26 \leq s \leq 30, \\ 10, & 31 \leq s \leq 35, \\ 9, & s \geq 36. \end{cases}$$

*Closing the Bounds for $\rho_{2,3}$ and $\rho_{3,2}$.* For the smallest parameters with $t \neq d$, Theorem 6 together with Theorem 5 and the values of [FFL26] determines $\rho_{3,2}$ and $\rho_{2,3}$ completely.

**Corollary 6.** *The values of $\rho_{3,2}(s)$ and $\rho_{2,3}(s)$ for $s \geq 7$ are given in Table 3.*

| $s$ | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14–16 | 17–20 | 21–34 | $\geq 35$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\rho_{3,2}(s)$ | 35 | 17 | 12 | 10 | 9 | 9 | 9 | 8 | 8 | 7 | 7 |
| $\rho_{2,3}(s)$ | 21 | 14 | 11 | 10 | 10 | 9 | 9 | 9 | 8 | 8 | 7 |

**Table 3.** Exact values of $\rho_{3,2}(s)$ and $\rho_{2,3}(s)$.

*Proof.* By Corollary 1 and Lemma 1, we have $\rho_{3,2}(7) = \binom{7}{3} = 35$, and $\rho_{3,2}(s) = 7$ iff $s \geq \binom{7}{2} = 21$. For $d = 3$, Corollary 5 gives $\rho_{3,2}(s) = 8$ for $14 \leq s \leq 20$ and

$\rho_{3,2}(s) \geq 9$ for $s \leq 13$. Moreover, $\rho_{3,2}(8) = 17$ by Theorem 5, and $\rho_{3,2}(9) = 12$, $\rho_{3,2}(10) = 10$ and $\rho_{3,2}(11) = 9$ by [FFL26], where the latter also gives $\rho_{3,2}(12) = \rho_{3,2}(13) = 9$ by Lemma 2. Finally, an $\mathrm{nc}(x, 2, 3, y)$ exists iff an $\mathrm{nc}(y, 3, 2, x)$ exists by Lemma 1, so $\rho_{2,3}(x) = \min\{y \mid \rho_{3,2}(y) \leq x\}$, which gives the values of $\rho_{2,3}$. □

## 5 Results from Computational Search

All upper bounds of this work, see Figure 1, are attained by explicit coverings, which we found by four complementary methods. Translate coverings and SAT models with prescribed automorphisms reach coverings with many points, as the symmetry reduces the size of the search space by roughly the group order, whereas simulated annealing finds coverings with few points and many members, where no symmetry can be expected. Every covering was verified independently by checking both conditions of Definition 1 by brute force, and we subsequently removed members with fewer than $t$ elements, repeated members, and members all of whose $t$-subsets are contained in other members, which preserves both conditions by Definition 1.

### 5.1 SAT Models with Prescribed Automorphisms

Given a group $G$ acting on $U_s$, we restrict the search for coverings invariant under $G$ by this method. Since both conditions of Definition 1 are invariant under automorphisms, it suffices to impose the covering condition for one representative of each $G$-orbit of $t$-sets, and non-completeness for one representative of each $G$-orbit of $d$-sets of members. Both are encoded with auxiliary variables, i.e. by a clause stating that some member contains the given $t$-set, and a clause stating that some point is missed by all members of the given $d$-set, and we solve the resulting instances with the CaDiCaL SAT solver [BFF+24]. As coverings without the prescribed symmetry are not found, this approach only yields upper bounds on $\rho_{t,d}(s)$.

Our first encoding extends the translate coverings of Section 3.2 by fixed points and additional multiplicative symmetry. Concretely, for integers $q, a, f \geq 0$, the point set consists of $a$ copies of $\mathbb{Z}_q$ together with $f$ fixed points, such that $s = aq + f$. For a subgroup $H$ of the unit group $\mathbb{Z}_q^*$, the group $G = \{x \mapsto ux + c \mid u \in H, c \in \mathbb{Z}_q\} \cong \mathbb{Z}_q \rtimes H$ acts simultaneously on each copy of $\mathbb{Z}_q$ and fixes the remaining points, where $H = \{1\}$ yields purely cyclic coverings. We search for $b$ base blocks $B_1, \ldots, B_b$, each invariant under multiplication by $H$ and encoded by one variable per $H$-orbit of points, and take as members all translates $B_i + c$ with $i \leq b$ and $c \in \mathbb{Z}_q$, possibly together with members that are unions of point orbits. For each $s$, we started from the smallest $r = bq$ admitted by the bounds of Section 2 and increased $b$ until a covering was found, trying all subgroups $H$ for each $b$. All new coverings for $(t, d) = (4, 3)$ with $20 \leq s \leq 26$, as well as $\mathrm{nc}(26, 3, 4, 100)$, were found in this way with $a = f = 1$.

Our second encoding is based on the Kramer-Mesner method, which is a standard combinatorial tool for constructing $t$-designs and Steiner systems with a prescribed automorphism group, see e.g. [KNP11,KKT+25,KV16]. By working with orbits instead of single sets, it reduces the existence problem to a much smaller integer system, and in contrast to our first encoding, it applies to arbitrary groups $G$. Here, we fix the $G$-orbits $\mathcal{M}_1, \ldots, \mathcal{M}_u$ of candidate members and introduce one variable $x_i$ per orbit. For a $t$-set $T$, the number of members of $\mathcal{M}_i$ containing $T$ only depends on the orbit of $T$, so the covering condition becomes $Ax \geq \mathbf{1}$ for the Kramer-Mesner matrix $A$, and the resulting covering has $\sum_i x_i|\mathcal{M}_i|$ members. In this way, we found e.g. $\mathrm{nc}(18, 3, 3, 18)$, whose automorphism group has order 64, and $\mathrm{nc}(10, 2, 4, 31)$, which admits an automorphism of order 21.

### 5.2 Exact SAT Model

To exclude small coverings, we directly encode the incidence matrix $X^{(\mathcal{C})}$ of an $\mathrm{nc}(s, t, d, r)$ by $sr$ variables, with both conditions encoded as above. The points and members may be permuted freely, which is why we additionally require both the rows and the columns of $X^{(\mathcal{C})}$ to be lexicographically non-increasing, which every 0/1-matrix satisfies after suitable permutations [FFH+02]. Moreover, we impose $t \leq |S_i| \leq s - (d-1)t - 1$ for every member and $\deg(p) \geq (t-1)d + 1$ for every point. The upper bound and the degree bound hold in every covering by Lemma 3, and the lower bound is no restriction, as a member with fewer than $t$ elements may be replaced by a copy of another member. Hence, an unsatisfiable instance proves that no $\mathrm{nc}(s, t, d, r)$ exists. As a consistency check, the model reproduces the nonexistence results of Theorem 5 and [FFL26], as well as the nonexistence of $\mathrm{nc}(13, 3, 2, 8)$ implied by Corollary 5.

### 5.3 Simulated Annealing

For few points and many members, we use simulated annealing on families of $r$ subsets of $U_s$. The cost of a family is the number of $t$-sets contained in no member plus the number of $d$-sets of members covering $U_s$, and a move adds or removes a single point of a single member, accepted with the Metropolis probability at the current temperature. Whenever the cost reaches zero, we have found an $\mathrm{nc}(s, t, d, r)$, remove one member and continue. In this way, we found nc(10,4,2,53) and nc(14,3,3,37), as well as an nc(12,3,3,60) and an nc(13,3,3,45), each of which contains a member all of whose 3-subsets lie in another member. Removing it yields nc(12,3,3,59) and nc(13,3,3,44). The automorphism group of nc(12,3,3,59) has order 2, while nc(10,4,2,53), nc(13,3,3,44) and nc(14,3,3,37) have trivial automorphism groups.

## 6 Open Problems

In this work, we narrowed the gap between the known lower and upper bounds on $\rho_{t,d}(s)$ for small parameters, by combining the development of new theoretical lower bounds with the computational search of explicit examples.

In order to gain a better understanding on the structure of minimal non-complete set coverings, the ones of main practical interest for threshold implementations, we conclude with two open questions on this.

1. *Regularity of minimal balanced coverings.* Does there always exist a $k$-regular $\mathrm{nc}(\nu_{\mathrm{bal}}, t, d, \nu_{\mathrm{bal}})$, in particular, is $\nu_{\mathrm{bal}}(t,d) = \nu_{\mathrm{reg}}(t,d)$ for all $t, d$? This is the case for all parameters settled so far, and it could be disproven by the existence of an $\mathrm{nc}(n, t, d, n)$ with $n < \nu_{\mathrm{reg}}(t,d)$.
2. *Twin points.* Since a minimal covering has pairwise distinct members, the dual of a minimal covering may still contain repeated members, which happens iff the covering contains two points lying in exactly the same members. Does there exist a minimal balanced covering with this property? Deleting one of the two points shows that this requires $\rho_{t,d}(\nu_{\mathrm{bal}} - 1) = \nu_{\mathrm{bal}}$, which by duality is impossible for $t = d$.

*Acknowledgements.* Enrico Piccione is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

*Use of AI.* We used ChatGPT-6 Astra and Claude Opus 5.5 for identifying the classical combinatorics literature linked to non-complete set coverings. Moreover, we used them to assist with computational investigations in Section 5, in verifying the correctness of theoretical results and in proofreading the manuscript. We declare full responsibility for the content of this work.

## References

AZN21. Victor Arribas, Zhenda Zhang, and Svetla Nikova. LLTI: low-latency threshold implementations. *IEEE Trans. Inf. Forensics Secur.*, 16:5108–5123, 2021.

BFF+24. Armin Biere, Tobias Faller, Katalin Fazekas, Mathias Fleury, Nils Froleyks, and Florian Pollitt. CaDiCaL 2.0. In *Computer Aided Verification: 36th International Conference, CAV 2024, Montreal, QC, Canada, July 24–27, 2024, Proceedings, Part I*, pages 133–152, Berlin, Heidelberg, 2024. Springer-Verlag.

BGHT03. Mieczysław Borowiecki, Jarosław Grytczuk, Mariusz Hałuszczak, and Zsolt Tuza. Schütte's tournament problem and intersecting families of sets. *Combinatorics, Probability and Computing*, 12(4):359–364, 2003. https://doi.org/10.1017/S0963548303005674.

BGN+14. Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Higher-order threshold implementations. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th*

*International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 326–343. Springer, 2014.

EL75. Paul Erdős and László Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. In A. Hajnal, R. Rado, and V. T. Sós, editors, *Infinite and Finite Sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II*, volume 10 of *Colloquia Mathematica Societatis János Bolyai*, pages 609–627. North-Holland, Amsterdam, 1975.

FFH+02. Pierre Flener, Alan M. Frisch, Brahim Hnich, Zeynep Kiziltan, Ian Miguel, Justin Pearson, and Toby Walsh. Breaking row and column symmetries in matrix models. In *Principles and Practice of Constraint Programming – CP 2002*, volume 2470 of *Lecture Notes in Computer Science*, pages 462–477. Springer, 2002.

FFL26. Oriol Farràs, Óscar Fidalgo, and Carlos Andres Lara-Nino. Non-complete set coverings for higher order threshold implementations. *Designs, Codes and Cryptography*, 94(5):113, 2026.

GL25. Vincent Grosso and Carlos Andres Lara-Nino. Overshooting the threshold: $(td + n)$-masking. *IACR Cryptol. ePrint Arch.*, 2025:1936, 2025.

GLN25. Vincent Grosso and Carlos Andres Lara-Niño. Leveraging the resources of modern FPGAs in the design of high-performance masked architectures. In *XVIII Reunión Española sobre Criptología y Seguridad de la Información: XVIII RECSI, León 23-25 octubre 2024*, pages 211–216. Universidad de León, 2025.

ISW03. Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, 2003.

KJJ99. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *Advances in Cryptology — CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer Berlin Heidelberg, 1999.

KKT+25. Michael Kiermaier, Vedran Krčadinac, Vladimir D. Tonchev, Renata Vlahović Kruc, and Alfred Wassermann. Some new Steiner designs $S(2, 6, 91)$. *Journal of Algebraic Combinatorics*, 62(2), September 2025.

KNP11. Vedran Krčadinac, Anamari Nakić, and Mario Osvin Pavčević. The Kramer–Mesner method with tactical decompositions: some new unitals on 65 points. *Journal of Combinatorial Designs*, 19(4):290–303, 2011.

KV16. Vedran Krčadinac and Renata Vlahović. New quasi-symmetric designs by the kramer–mesner method. *Discrete Mathematics*, 339(12):2884–2890, 2016.

NRR06. Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold implementations against side-channel attacks and glitches. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *Information and Communications Security, 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006, Proceedings*, volume 4307 of *Lecture Notes in Computer Science*, pages 529–545. Springer, 2006.

Pet19. George Petrides. On non-completeness in threshold implementations. In Begül Bilgin, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Proceed-*

*ings of ACM Workshop on Theory of Implementation Security, TIS@CCS 2019, London, UK, November 11, 2019*, pages 24–28. ACM, 2019.

PR17. Joanna Polcyn and Andrzej Ruciński. A hierarchy of maximal intersecting triple systems. *Opuscula Mathematica*, 37(4):597–608, 2017. https://doi.org/10.7494/OpMath.2017.37.4.597.

Sch64. J. Schönheim. On coverings. *Pacific Journal of Mathematics*, 14(4):1405–1411, 1964.