

Gábor CZÉDLI

June 21, 2023

Generating quasiorder lattices and some other lattices by few elements

Presented at the online part of the 15th International Summer School-Conference
"Problems Allied to Universal Algebra and Model Theory", Novosibirsk - Erlagol

This is the pdf version. During the talk,
Xournal++ (version 1.1.3) (*/ˌzəʊnəlˌplʌsˈplʌs/*), a free
and open-source note-taking software was running.

(1)

<http://www.math.u-szeged.hu/~czedli/>

The screenshot shows a website header for Gábor Czédli. On the left, there are navigation links: 'Home', 'Magyarul' (with a Hungarian flag icon), 'Research:', 'My publications', 'Conference talks', and '"Popular" math. talks'. On the right, the name 'Gábor CZÉDLI' is displayed in large bold letters, followed by his titles: 'professor emeritus, doctor of mathematical science'. Below this, his affiliation is listed: 'Department of Algebra and Number Theory, Bolyai Institute, University of Szeged, Szeged, Aradi vértanúk tere 1, Hungary - 6720.' Two pink arrows point from the left side to the 'Research:' and 'Conference talks' links.

(2)

Conjecture/hint: if a finite algebra (i.e., general algebraic system
 --- is large enough (i.e., it consists of very many elements),
 --- its basic operations are easy to perform (fast, by a computer),
 --- it is generated by few elements, and
 --- a random small subset is a generating set with high probability,
THEN the application of this algebra in cryptography has a chance.

(3)

Therefore: even though this talk deals with lattices, similar investigations with other types of algebras seem to be possible.

References:

- Delbrin Ahmed and CzG: (1+1+2)-generated lattices of quasiorders. ASM 2021, pp 415–427**
- I. Chajda and CzG: How to generate the involution lattice of quasiorders?, Studia Sci. M.Hung 1996, pp 415-427**
- CzG: Lattice generation of small equivalences of a countable set. Order 13 (1996), 11–16**
- CzG: Four-generated large equivalence lattices. ASM 1996, pp 47–49**
- CzG: (1+1+2)-generated equivalence lattices, J. Algebra, 221 (1999), 439–462**
- CzG: Four-generated quasiorder lattices and their atoms... Comm.Alg. (2017) pp.4037-4049**
- CzG: Four-generated direct powers of partition lattices and authentication. Publ.Debrecen(2021)447-472**
- CzG: Generating some large filters of quasiorder lattices. arXiv:2302.13911**
- CzG: Generating Boolean lattices by few elements and a protocol for authentication and cryptography based on an NP-complete problem. arXiv: http:2303.10790**
- CzG and J.Kulin: A concise ... lattices of quasiorders and transitive relations. ASM(2017) pp.3-12**
- CzG and Lillian Oluoch: Four-element gen. sets ... and their direct products. ASM(2020) pp.405-448**
- T.Dolgos (M.Maróti's student): Gen. equ. and quasiorder lattices over finite sets. BSc Thesis, SZTE 2015**
- J. Kulin: Quasiorder lattices are five-generated. Discuss. Math. Gen. Alg. Appl.=2016) 59-70**
- Lillian Oluoch and Amenah Al-Najafi: Discuss. Math. Gen. Algebra and Appl. 42(2022) 327–338**
- H. Strietz: Finite partition lattices are four-generated. Proc. Lattice Th. Conf. Ulm, 1975, pp 257-259**
- G.Takách: Three-generated quasiorder lattices. Discuss. Math. Alg.& Stoch.(1996) pp. 81-98**
- Vilmos Totik: Oral communication. Somewhen in the nineties.**
- L. Zádori: Generation of finite partition lattices. Lectures in universal algebra (Proc. Colloq.Szeged, 1983),North-Holland, 1986,pp. 573–586.**

 } most of this talk

What is a lattice?

$(L; \vee, \wedge)$

$(L; \leq)$ such that for all $x, y \in L$, $\exists \sup\{x, y\}$ and $\exists \inf\{x, y\}$.

If $\sup X$ and $\inf X$ exist for every subset $X \subseteq L$, then L is a *complete lattice*.

Examples: for a given set A , the reflexive, symmetric and transitive relations of A are called the *equivalences* of A . They form the *equivalence lattice* of A : $\mathcal{E}(A) = (\mathcal{E}(A); \subseteq)$.

Similarly, the reflexive and transitive relations of A are called the *quasiorders* (or pre-orders) of A . They form the *quasiorder lattice* of A : $\mathcal{Q}(A) = (\mathcal{Q}(A); \subseteq)$.

In both cases, the meet \wedge in the lattice is the set-theoretic intersection while the join \vee is the transitive closure of the set-theoretic union.

If $\kappa := |A|$, the cardinality of A , then we often write $\mathcal{E}(\kappa)$ and $\mathcal{Q}(\kappa)$ instead of $\mathcal{E}(A)$ and $\mathcal{Q}(A)$, respectively.

Part 1. Generating quasiorder lattices and equivalence lattices

Definition: Let $n \in \mathbb{N}^+$. We say that a complete lattice L is n -generated if there is a subset $X \subseteq L$ such that

- $|X| \leq n$, and
- X generates L as a complete lattice. That is, whenever S is a subset of L closed with respect to arbitrary (not only finitary) meets and joins and $X \subseteq S$, then $S = L$.

Of course, for a finite L , nothing is unusual here; then X generates L if the only sublattice of L that includes X is L itself.

Shortly saying: “ n -generated” means that “generated by n or fewer elements”.

$\text{mg}(L)$ denotes the smallest n such that L is n -generated.

Definition: a cardinal number μ is *inaccessible*, if

- whenever $\nu < \mu$, then $2^\nu < \mu$, and
- whenever I is a set of cardinal numbers such that $|I| < \mu$ and, for every $\nu \in I$, $\nu < \mu$, then $\sum_{\nu \in I} \nu < \mu$.

We call a cardinal number κ *accessible* if there exists no inaccessible μ such that $\mu \leq \kappa$.

$n \in \mathbb{N}^+$: Zádori(1983), Strietz(1975): $\mathcal{E}(n)$ is 4-generated.

$\kappa_0 := \aleph_0, \kappa_{n+1} := 2^{\kappa_n}$. Chajda and Czédli (1996): if $\lambda \leq \kappa_n$, then $\mathcal{Q}(\lambda)$ is 3^* -generated and so 6-generated.

Czédli(1996): $\mathcal{E}(\lambda)$ is 4-generated provided that λ is accessible ($\forall \lambda$ is such in Kuratowski's model of ZFC).

Takách (1996): if λ is *accessible* then $\mathcal{Q}(\lambda)$ is 3^* -generated and so 6-generated.

Dolgos (2015): if $\lambda \leq \aleph_0$, then $\mathcal{Q}(\lambda)$ is 5-generated.

Kulin (2016): for λ accessible, $\mathcal{Q}(\lambda)$ is 5-generated.

Czédli–Kulin (2017) $4 \neq \lambda$ is accessible $\Rightarrow \mathcal{Q}(\lambda)$ is 4-generated.

Czédli (2017): if $3 \leq \lambda$, then $\mathcal{Q}(\lambda)$ is **not** 3-generated.

For almost \forall accessible λ , $\mathcal{Q}(\lambda)$ and $\mathcal{E}(\lambda)$ are (1+1+2)-generated:

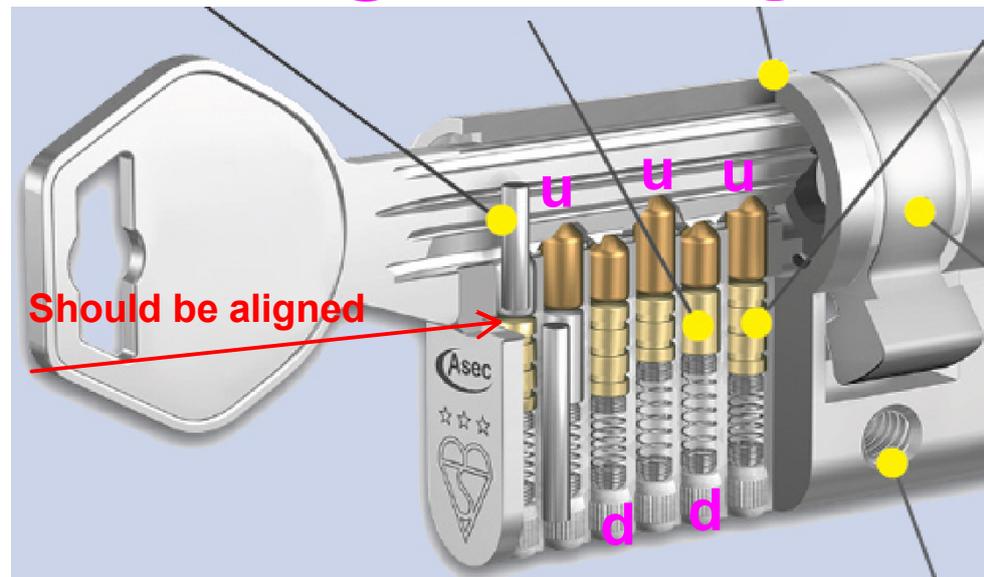
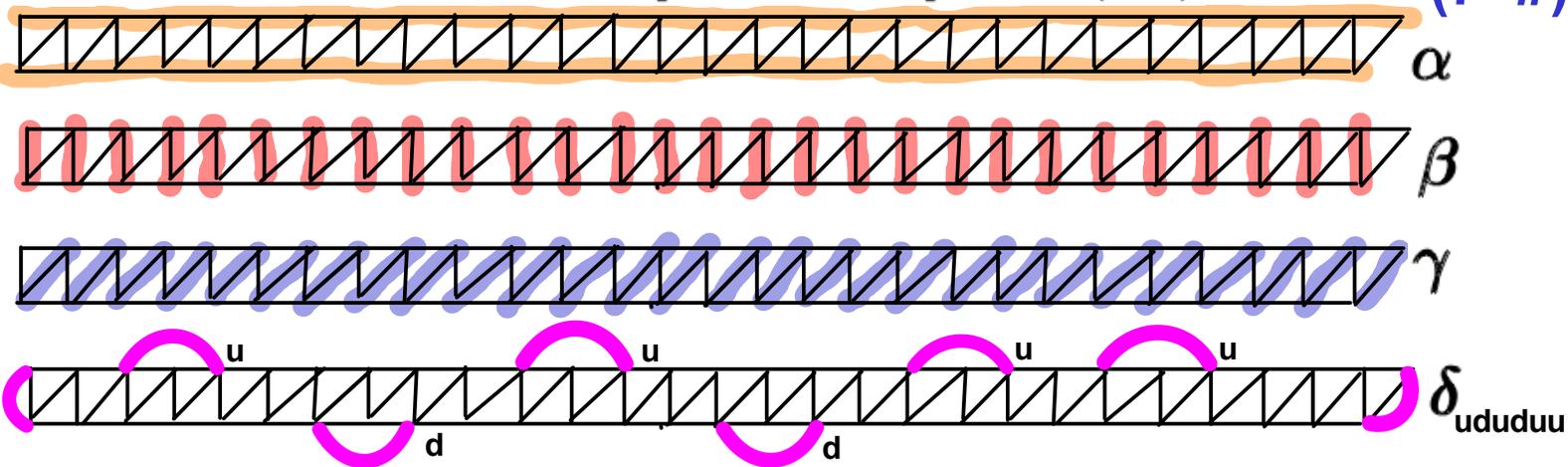
Strietz, Zádori, Czédli, Kulin, Delbrin Ahmed, Lillian Oluoch.

Tran(λ) is 8-generated for $\lambda \leq \aleph_0$ by T. Dolgos; it is 6- and 3^* -generated for λ accessible by Czédli and Kulin (2017)

Many open problems, e.g., is $\mathcal{Q}(4)$ 4-gen.? For $n \in \{4, 5, 7, 8, 9, 10, 12\}$, is $\mathcal{Q}(n)$ (1+1+2)-gen.? Reduce “ 3^* -”? Inaccessible λ ?

(V. Totik proved that my method does not work for an inaccessible $\lambda \dots$)

Zádori's generators: $[\alpha, \beta, \gamma, \delta] = \mathcal{E}(57)$ (7 #)



Some other tricks are also needed.

Even $\mathcal{E}(100)^{3 \cdot 10^{89}}$ is 4-generated. $\mathcal{E}(100)$ has many 4-element generating sets.

An excerpt from Czédli and Oluoch's paper (2000):

Proof of Theorem 4.4. In addition to earlier experience with generating sets of partitions lattices, see the References section, an idea is also borrowed from locksmithing. In a traditional pin tumbler cylinder lock, there are pins of different (to be more precise, not necessarily equal) lengths, and a key can turn the plug if and only if the heights of its ridges match these lengths. The $\sum\{[I_i^\varphi]^e : x_i = 1, 1 \leq i \leq m\}$



4.4. In addition to earlier experience the References section, an idea is borrowed from locksmithing. In a traditional pin tumbler cylinder lock, there are pins of different (to be more precise, not necessarily equal) lengths, and a key can turn the plug if and only if the heights of its ridges match these lengths. The

| n | 4 | 5 | 6 | 7 | 8 | 9 |
|-----------------|------------|------------|-------------|------------|---------|------------------------|
| $100p(n)$ | 3.6630037 | 1.9595531 | 1.613014768 | | | |
| N | 10 000 000 | 10 000 000 | 10 000 000 | 15 000 000 | 500 000 | 25 000 |
| time | 8 minutes | 27 min | 3h+33min | 102 hours | 95 h | 166 h \approx a week |
| s | 367 221 | 196 243 | 161 768 | 238 223 | 8 244 | 438 |
| $100\hat{p}(n)$ | 3.67221 | 1.96243 | 1.61768 | 1.58815 | 1.64880 | 1.75200 |

Percentages of the generating ones among the 4-element subsets of $\mathcal{E}(n)$; the paper contains some other tables and confidence intervals, too.

G. Czédli: Four-generated direct powers Publicationes Math. (Debrecen) 99 (2021), 447–472.

| n | 4 | 5 | 6 | 7 | 8 | 9 |
|---------------------------|---------|-------------------|----------------------|----------------------|----------------------|----------------------|
| $ \text{Part}(n) $ | 15 | 52 | 203 | 877 | 4 140 | 21 147 |
| $ \forall 8\text{-sets} $ | 6435 | $7.53 \cdot 10^8$ | $6.22 \cdot 10^{13}$ | $8.41 \cdot 10^{18}$ | $2.13 \cdot 10^{24}$ | $9.91 \cdot 10^{29}$ |
| $ \text{tested} $ | 100 000 | 10 000 | 10 000 | 6000 | 1000 | 284 |
| $ \text{found} $ | 89 780 | 7 690 | 7913 | 5044 | 848 | 248 |
| % | 89.78 | 76.90 | 79.13 | 84.01 | 84.80 | 90.19 |

The same percentages for 8-element subsets of $\mathcal{E}(n)$.

For a poset $P = (P; \leq)$, $\mathcal{Q}^*(P)$ is the lattice of those quasiorders of P that extend " \leq_P "; it is a filter of $\mathcal{Q}(A)$.

$\mathcal{Q}^*(P)$ is a filter of $\mathcal{Q}(P)$.

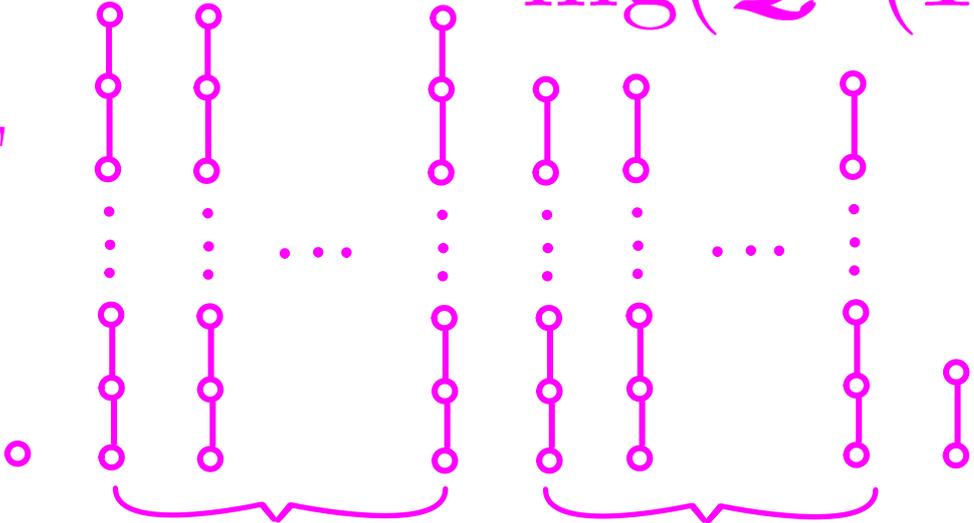


P is a chain
of length
 $4 \cdot 10^9$
(four billion)

$\text{mg}(\mathcal{Q}^*(P)) = ?$ **35**

$\text{mg}(\mathcal{Q}^*(T)) = ?$

T



I do not know.

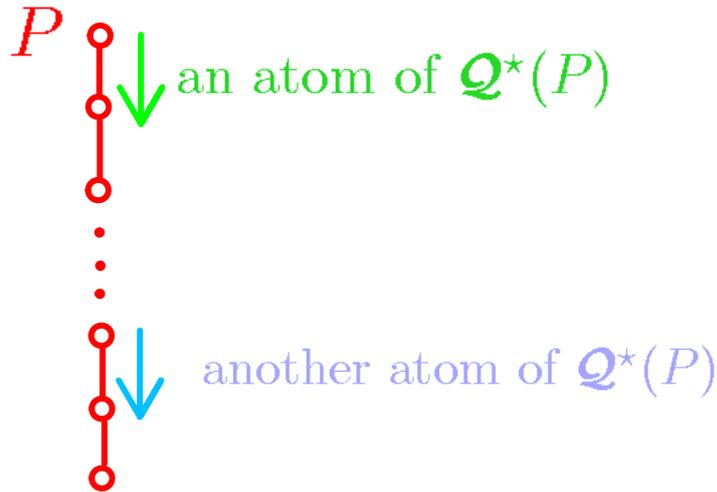
I only know that

\leq **43**

ten billion chains of length four billion

six billion chains of size four billion, i.e., of length 4 billion minus 1

Czédli: Generating some large filters (2023) arXiv:2302.13911 (#11)
proves more; here I prove only: **Theorem: = 35 and ≤ 43 .**



Dongseok Kim, Young Soo Kwon, and Jaeun Lee (2014)

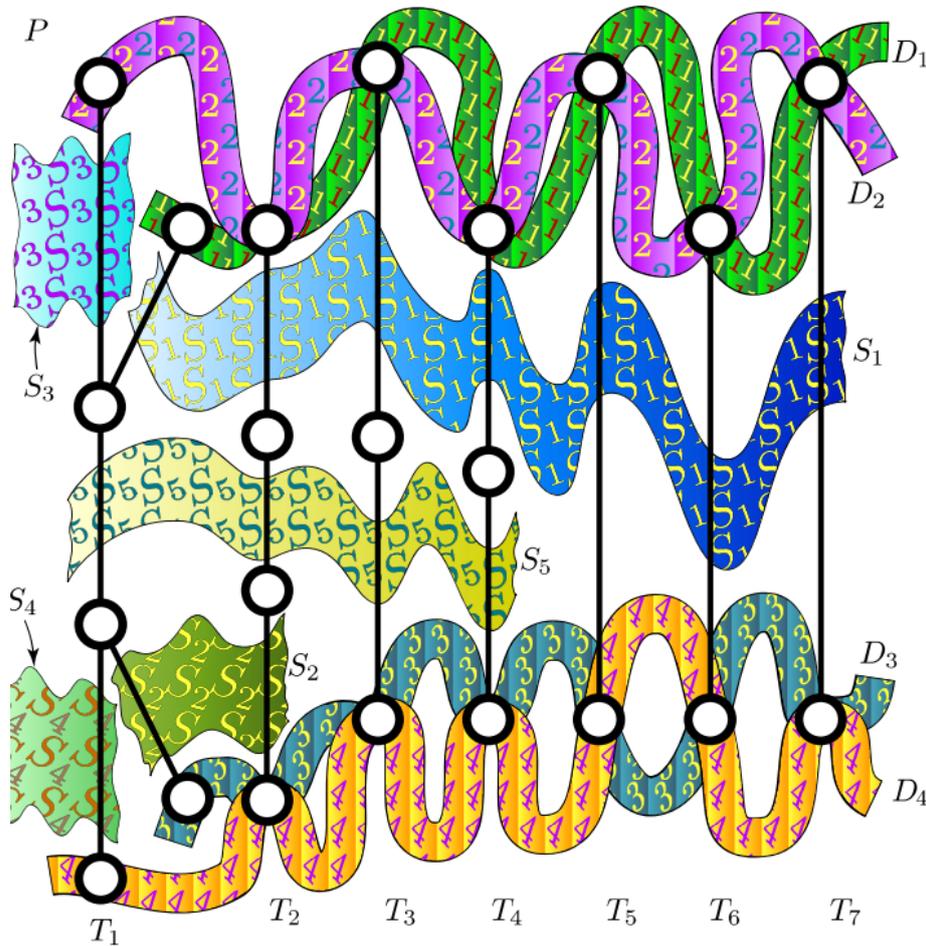


$\mathcal{Q}^*(P) \cong B_{4\,000\,000\,000}$,
the Boolean lattice with 4 000 000 000
atoms, so we have reduced the problem
to another problem, which comes next.

This proves the “=35” part of the theorem.
The rest of the proof is omitted.

The paper takes care of more involved posets, too. E.g.:

(#12)



(The figure captures some idea of the proof, not explained here.)
For *this* poset P ,
when $|Q^*(P)| > 9 \cdot 10^{13}$,
the theorem asserts that
 $\text{mg}(Q^*(P)) \leq 22$.

Part 2. Authentication and cryptography

(#13)

For $\vec{h} = (h_1, \dots, h_k) \in B_n^k$, this k -dimensional vector is *generating* if $[h_1, \dots, h_k] = B_n$.

We shall soon see that $\text{mg}(B_{1000}) = 13$. So B_{1000} has a 13-dimensional generating vector. As $k > 13$ grows, B_{1000} has more and more k -dimensional generating vectors.

| | | | | |
|--------|-------|---------------|--------------------|---------------|
| n=1000 | k=40 | Tested:100000 | Generating: 42; | 506.867 sec |
| n=1000 | k=50 | Tested:100000 | Generating: 59003; | 1305.780 sec |
| n=1000 | k=50 | Tested:100000 | Generating: 59162; | 10965.266 sec |
| n=1000 | k=60 | Tested:100000 | Generating: 96878; | 1967.896 sec |
| n=1000 | k=70 | Tested:100000 | Generating: 99823; | 2321.272 sec |
| n=1000 | k=80 | Tested:100000 | Generating: 99990; | 2647.147 sec |
| n=1000 | k=90 | Tested:100000 | Generating: 99999; | 2974.364 sec |
| n=1000 | k=100 | Tested:100000 | Generating:100000; | 3265.869 sec |

The program chose one hundred thousand random k -dimensional vectors and counted the generating ones among them.

When no anonymous usage is permitted: **secret key** cryptography and authentication are used. In our model:

(14 #)

Kate communicates with her Bank.

Let, say, $k := 300$, $n := 1000$, and $t := 100$.

Secret key: a k -dimensional generating vector

$\vec{h} = (h_1, \dots, h_k) \in B_n^k$ of B_n .

$\vec{p} = (p_1, \dots, p_t)$: a vector of k -ary lattice terms.

Protocol: The Bank sends a random \vec{p} to Kate and she sends $\vec{p}(\vec{h}) \in B_n^t$ back. And vice versa. $\vec{p}(\vec{h})$ is also used as a key of Vernam's cipher.

Adversary: intercepts and/or sends messages. As \vec{p} is always new, he cannot use an intercepted $\vec{p}(\vec{h})$ again. As $\vec{p}(\vec{h})$ can take $|B_n|^t = 2^{nt}$ many values, he cannot find a valid $\vec{p}(\vec{h})$ by chance unless he can solve the equation $\vec{p}(\vec{x}) = \vec{c}$, where $\vec{c} := \vec{p}(\vec{h}) \in B_n^t$ is an intercepted constant with the corresponding intercepted vector \vec{p} of lattice terms and $\vec{x} \in B_n^k$ (playing the role of \vec{h}) is the unknown.

unless he can solve $\vec{p}(\vec{x}) = \vec{c}$, where $\vec{c} := \vec{p}(\vec{h}) \in B_n^t$ and $\vec{x} \in B_n^k$ (15 #)

Observation: even if $n = 1$ and $t = 2$, solving $\vec{p}(\vec{x}) = \vec{c}$ is an NP-complete problem.

We skip over the following easy proof in the talk.

Proof: Suppose for contradiction that \exists a polynomial f and an algorithm Γ such that for \forall input $\vec{p}(\vec{x}) = \vec{c}$ of size s , if this input has a solution for \vec{x} , then Γ finds a solution in $f(s)$ time.

Then we can solve the 3COLOR as follows. Let G be a simple graph of size s_1 . For each vertex i , take the *color variables* r_i , w_i , and g_i . For each edge $e: i \text{---} j$, we take:

$$\left. \begin{array}{l} \Phi_e : (r_i \vee w_i \vee g_i) \wedge (r_j \vee w_j \vee g_j) = 1 \text{ and } \text{nonempty} \\ \Psi_e : (r_i \wedge r_j) \vee (w_i \wedge w_j) \vee (g_i \wedge g_j) = 0. \text{ disjoint} \end{array} \right\} \text{color sets}$$

$$\text{Let } p_1 := \bigwedge_{e \in \text{Edge}(G)} \Phi_e, \quad p_2 := \bigvee_{e \in \text{Edge}(G)} \Psi_e, \quad \vec{p} = (p_1, p_2).$$

Let $\vec{x} := (\dots, r_i, w_i, g_i, \dots)$. Let s be the size of $\vec{p}(\vec{x}) = (1, 0)$.

Then $s = \text{const} \cdot s_1$. **Run** Γ for the red input in $f(s)$ steps.

After at most $f(s)$ many steps, stop Γ . Then print “YES, G is 3-colorable” if Γ found a solution in that many steps, and print “NO” otherwise. This “magenta algorithm” needs

$\approx 2f(s) = 2f(\text{const} \cdot s_1)$ steps, which is a polynomial of s_1 .

(Factor 2: since we need to count the steps of Γ .)

We have solved 3COLOR in polynomial time. Q.e.d.

The value of NP-completeness: Even though we can prove that the underlying problem (to solve the equation \vec{x} from $\vec{p}(\vec{x}) = \vec{c}$ for the unknown \vec{x}) is NP-complete and so it is NP-hard,

this fact may encourage us to do further research,

but the NP-hardness of the underlying problem in itself is NOT ENOUGH to secure a cryptosystem.

First, because an NP-hard problem can have many easy instances, and we should guarantee that our protocol avoids these easy instances almost surely.

Second, if, say, $n = 1$ and $t = 2$, then the underlying problem is still NP-hard but the adversary need not break it; he need not solve the equation! He only needs to present $t = 2$ bits! At every 4th random trial, he can empty Kate's bank account!

Fortunately, for n big, $\vec{p}(\vec{h})$ can take $(2^n)^t$ many values. Hence, the Adversary can hardly find the right one accidentally.

The protocol works with, say $\mathcal{E}(400)$ or $\mathcal{Q}(200)$ instead of B_{1000} . **Warning:** in spite of my heuristic ideas, the security is not proved; further analysis would be necessary. (Note that some cryptographic protocols are based only on heuristic ideas rather than rigorous mathematical proofs.)

Czédli: Four-generated direct powers of partition lattices and authentication. Publ.Debrecen(2021)447-472

Czédli: Generating Boolean lattices by few elements and a protocol for authentication and cryptography based on an NP-complete problem. arXiv: <http://2303.10790> (2023)

Part 3. Generating Boolean lattices with few elements (17#)

Monster := $B_{112\ 186\ 277\ 816\ 662\ 845\ 432}$ **mg(Monster)=70**
(Subscript $\approx 1.12 \cdot 10^{20}$) What is $\text{mg}(\text{Monster})$?

$$\text{Sp}(n) := \binom{n}{\lfloor n/2 \rfloor}$$

, let $\text{LASp}(n)$ be the smallest $k \in \mathbb{N}^+$ such that $n \leq \text{Sp}(k)$.

Sp comes from "Sperner", LASp from "Left Adjoint of Sperner function."

Theorem. For $n \in \mathbb{N}^+$, $\text{mg}(B_n) = \text{LASp}(n)$.

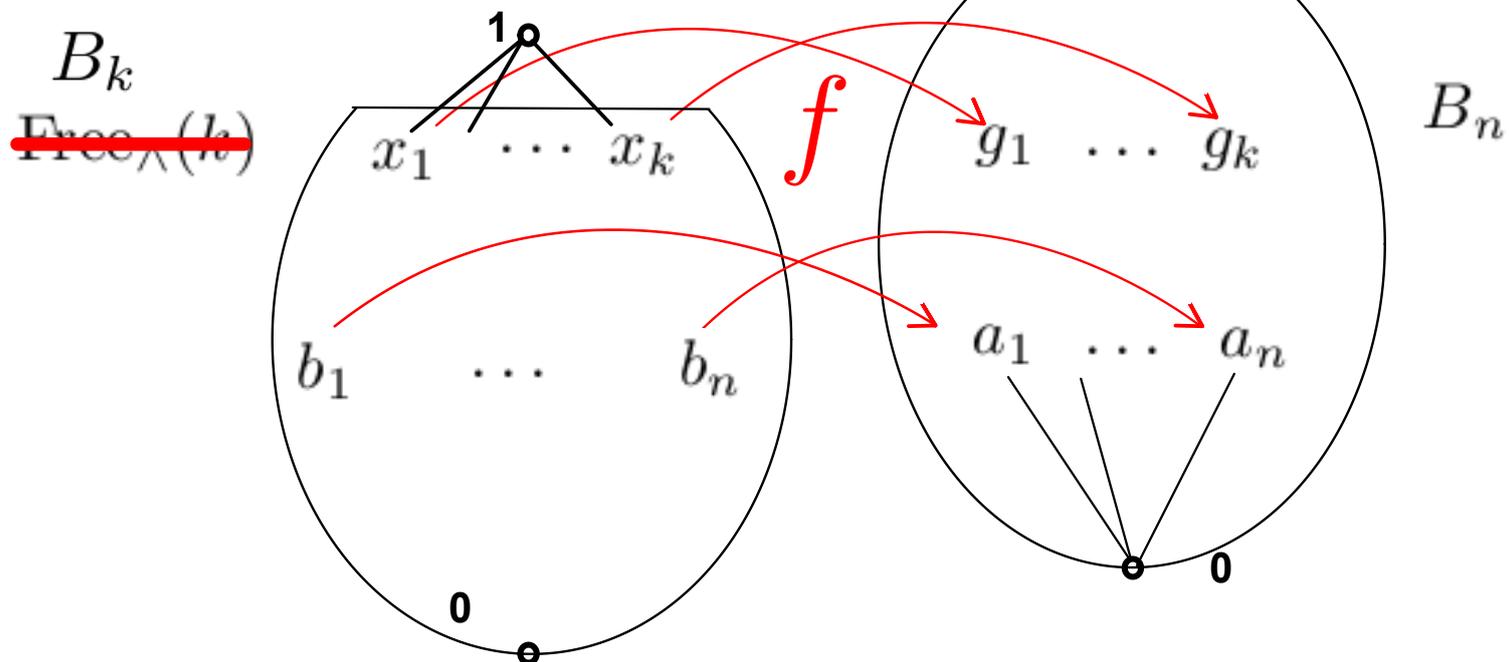
CzG: Generating Boolean lattices by few elements and a protocol for authentication and cryptography based on an NP-complete problem. arXiv: [http:2303.10790](http://arxiv.org/abs/2303.10790)

2023

If I still have time, let us see the proof in the next two slides.

Proof (necessity):

(18#)



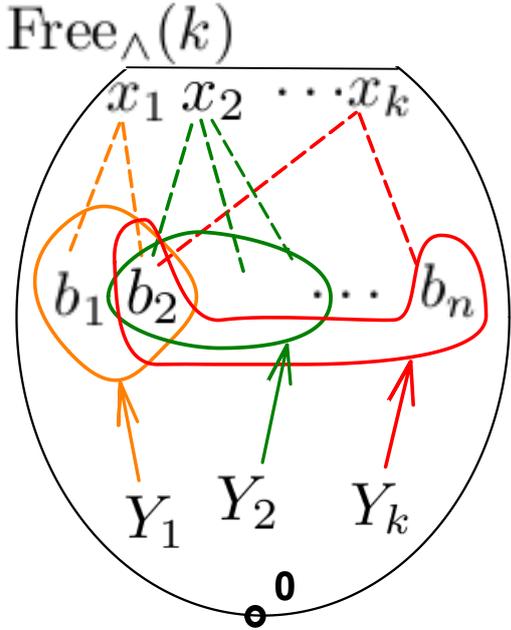
DNF $\Rightarrow a_1 = \bigvee \bigwedge g_{ij} = \bigwedge g_j$. So $a_1 \in [g_1, \dots, g_k]_{\wedge}$.
 Hence $a_1 \in f(\text{Free}_{\wedge}(k))$. Thus $\exists b_1$ such that $f(b_1) = a_1$.
 As the a_i 's form an antichain, so do the b_j 's.

Sperner's thm. $\Rightarrow n \leq \text{Sp}(k)$. \checkmark

(19#)

Sufficiency. For $n' < n$, $\exists B_n \twoheadrightarrow B_{n'}$. So we can assume $n = \text{Sp}(k)$ rather than " \leq ". Taking the meet of $\lfloor k/2 \rfloor$ free generators in \forall ways, we get an $\text{Sp}(k) = \binom{k}{\lfloor k/2 \rfloor} = n$ -element antichain $\{b_1, \dots, b_n\} \subseteq \text{Free}_\wedge(k)$.

<http://www.math.u-szeged.hu/~czedli/>



Let $Y_j := \{b_i : b_i \leq x_j\}$ for $j = 1, \dots, k$. In particular, $Y_2 := \{b_i : b_i \leq x_2\}$. Let $H_\ell := \bigcap \{Y_j : b_\ell \in Y_j\}$. E.g., $H_2 := \bigcap \{Y_j : b_2 \in Y_j\}$. Clearly, $\{b_2\} \subseteq H_2$.

For contradiction, suppose $b_3 \in H_2$. So $b_3 \in \bigcap \{Y_j : b_2 \in Y_j\}$. I.e., $\forall j, b_2 \in Y_j \Rightarrow b_3 \in Y_j$. I.e., $\forall j, b_2 \leq x_j \Rightarrow b_3 \leq x_j$.

Thank you for your attention.

So $b_2 = \bigwedge \{x_j : b_2 \leq x_j\} \geq \bigwedge \{x_j : b_3 \leq x_j\} = b_3$; contradiction. Thus $\{b_2\} = H_2$, whence $\{b_2\}$ belongs to $[Y_1, \dots, Y_k]$. So do each of $\{b_1\}, \dots, \{b_n\}$. So $\{Y_1, \dots, Y_k\}$ generates $\text{Pow}(\{b_1, \dots, b_n\}) \cong B_n$, q.e.d.