Reduction and efficient solution of MILP models of mixed Hamming packings yielding improved upper bounds

Péter Naszvadi[1,2] Mátyás Koniorczyk[1]

[1]Wigner Research Centre, Budapest, Hungary

[2]Faculty of Informatics, Loránd Eötvös University, Budapest, Hungary

GPU Day,
Budapest, 2024.05.30-31.

PROJECT FINANCED FROM THE NRDI FUND

Outline

- Ising, NISQ devices, annealers
- QUBO (UBQP)
- Hamming packings
- Development
- Discussion, conclusions

PROJECT FINANCED FROM THE NRDI FUND

Ising model

Ising

$$E(\mathbf{s}) = \sum_{(i,j)} J_{i,j} s_i s_j + \sum_j h_j s_j$$

- $s_i = \pm 1$ spins
- $p_{\mathbf{s}}(T) \propto \exp(-E(s)/T) \quad (\hbar = k_{\mathrm{B}} = 1)$
- $T = 0$: energy minimum

Adiabatic quantum computing

- initially: $\hat{H}_{\mathrm{init}}$: easily prepared, stable
  typically $\propto \sum_i \sigma_i^{(x)}$
- target: $\hat{H}_{\mathrm{obj}}$: encodes the objective; a ground state $|\phi\rangle$ is sought for.
- Evolve for *a long enough* T :

$$s = t/T, \quad \hat{H}(s) = (1-s)\hat{H}_{\mathrm{init}} + s\hat{H}_{\mathrm{obj}}$$

- Success probability

$$\mathrm{pr}(T) = |\langle\phi|\psi(T)\rangle|^2$$

- *Adiabatic theorem:* If done *slow enough*, and there is a gap for all s,

$$\mathrm{pr}(T) \to 1 \quad T \to \infty$$

E. Ising Beitrag zur Theorie des Ferro- und Paramagnetismus. Dissertation, Mathematisch-Naturwissenschaftliche Fakultät der Hamburgischen Universität Hamburg, 1924.

A. M. Childs, E. Farhi, & J. Preskill, Phys. Rev. A, **65**, 012322, (2001)

PROJECT FINANCED FROM THE NRDI FUND

Quantum annealing, NISQ

Adiabatic quantum computing + finite temperature (noise)

- A similar evolution (c.f. L. C. Venuti *et al.* Phys. Rev. A **93** 032118 (2016))
- The bigger the system, the more noise
  (c.f. Albash & Lidar, Rev. Mod. Phys. **90**, 015002 (2018))
- Probabilistic heuristics
- Multiple runs: Samples
- Not universal even ideally, but
  can be useful in some problems

NISQ

- Order of thousand of physical qubits
- Noisy
- Analog device (accuracy, scale)

e.g D-Wave

Ising vs. QUBO

QUBO (UBQP)

$$\min_{\mathbf{x}\in\{0,1\}^N} \mathbf{x}^\top Q \mathbf{x}$$

Affine transformation: $s_i = 2x_i - 1$

QUBO to Ising

$$h_i = \frac{Q_{i,i}}{2} + \sum_{j=1}^{n} \frac{Q_{i,j}}{4}$$

$$J_{i,j} = \frac{Q_{i,j}}{4}$$

Ising to QUBO

$$Q_{i,i} = 2\left(h_i - \sum_{j=1}^{n} J_{i,j}\right)$$

$$Q_{i,j} = 4J_{i,j}$$

PROJECT FINANCED FROM THE NRDI FUND

Hamming packings - introducing classic models for $N(H;d)$

- Any Hamming packing problem can be formulated as a disjunctive programming MIP problem
- These kind of MIP problems are basically weighted independent set problems
- Weighted independent set problems are (upper triangular) QUBO problems with
  - nonpositive diagonals
  - above diagonals' nonzero elements are all positive and dominate corresponding diagonal values

PROJECT FINANCED FROM THE NRDI FUND

Hamming packings II

Definition: Hamming space

$H \stackrel{\text{def}}{=} \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}$, with $\infty > k_1 \geqslant k_2 \geqslant \cdots \geqslant k_{n-1} \geqslant k_n \ (\geqslant 2)$

Definition: Hamming distance

$d(v, w) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \left(1 - \delta_{v[i], w[i]}\right)$

Example: $d(0101010101, 1010101010) = 10$ - p.ex. these words' Levenshtein distance is only 2!

Definition: Hamming packing

A subset of $H (C \subseteq H)$ for a given fixed $d \in \mathbb{N}$, where:
$\forall v \neq w \in C : d(v, w) \geqslant d$

PROJECT FINANCED FROM THE NRDI FUND

Importance, applications

- Football pool systems
- Sport betting systems (e.g. number of goals per participant)
- Telecommunication protocols, ECC
- Quality assurance

Hamming packings IV

One of the key questions is the maximal Hamming packing problem. Addressing the key question: what is the densest subset of a given space that keeps a minimal distance?

Definition: Maximal Hamming packing - cardinality

$$N(H;d) \stackrel{\text{def}}{=} \max\{|C| : C \subseteq H, \forall v \neq w \in C : d(v,w) \geqslant d\}$$

Other widely accepted notations:

- $N_q(n;d)$, when $H = \mathbb{Z}_q^n$
- $N(n;d)$, when $H = \mathbb{Z}_2^n$
- $N(b,t;d) = N_{2,3}(b,t;d)$, when $H = \mathbb{Z}_2^b \times \mathbb{Z}_3^t$

PROJECT FINANCED FROM THE NRDI FUND

Hamming packings V

Binary programming model for determining $N(H, d)$

$$\begin{aligned} \max \quad & \sum_{v \in H} x_v \\ s.t. \quad & x_v + x_w \leqslant 1 \quad \forall v,w \in H: 1 \leqslant d(v,w) \leqslant (d-1) \\ & \mathbf{x} \in \{0,1\}^n \quad . \end{aligned} \tag{1}$$

Properties

- The objective ensures the maximality of the chosen subset
- the constraints act as a mutex
- corresponding QUBO model is straightforward
  - A trick: DECOMPOSITION! (problem-specific, correctness?)

Hamming packings VI

QUBO model for determining $N(H;d)$

$$
\begin{array}{rl} -\min & \mathbf{x}^\top Q\mathbf{x} \\ & \mathbf{x} \in \{0,1\}^n \end{array} . \qquad (2)
$$

Where $Q \in \mathbf{R}^{n\times n}$ an upper-triangular matrix with all (-1) diagonals, and the above diagonal elements are given $P > 2$ penalty values iff there is a corresponding edge in the conflict graph.

- Q is a scaled adjacency matrix with filled diagonals
- the optimum is $N(H;d)$
- no need for helper variables when modeling such packing problems

PROJECT FINANCED FROM THE NRDI FUND

State-of-the-art records and yet unsolved Hamming packings

Key task

Find a mininal size model family that is still challenging and has many yet open problems.

Development I

Theorem

Every Hamming packing C with minimal distance d can be transformed to another Hamming packing C' with the same number of codewords and minimal distance, whose contact graph $CG(C')$ is connected.

Corollary

- can be add custom ball-squeezing constraints for a $N(H;d)$ MILP model
- yields maximal codes having contact graphs containing a full matching and for odd cardinality, a cherry too
- additionally to/instead of constraints, several initial codewords can be forced in the packing lookup model
  - $N(H;d)$ - without the loss of generality the assumption is correct to branch on pruning the contact graph in all distinct ways considering the fixed initial codewords

Development II

The desired transformation can be carried out using the following algorithm:

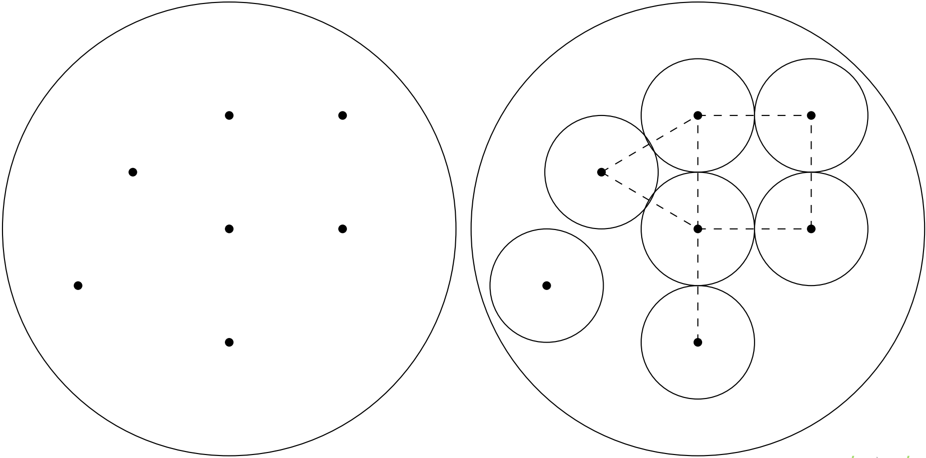
Algorithm 1 Transforming C to C' with the same number of codeword and minimal distance, and connected $CG(C')$

INPUT: $C \subseteq H$ nonempty Hamming packing, $d \in \mathbb{Z}, d > 0$ distance
START
pick a random $\hat{w} \in C$, them partition $C := C_1 \bigcup^* C_2$, where $C_1 = \{\hat{w}\}$ and $C_2 = C \setminus C_1$
while $C_2 \neq \emptyset$ **do**
  while $\exists w, w' : w \in C_1, w' \in C_2 : d(w, w') = d$ **do**
    update $C_1 : C_1 := C_1 \bigcup^* \{w'\}$
    update $C_2 : C_2 := C_2 \setminus \{w'\}$
  end while
  if $(C_2 \neq \emptyset)$ and $(d(C_1, C_2) \neq d)$ **then**
    sort increasing the elements of C_2 on distance of C_1
    let d' denote: $d' := d(C_1, C_2)$
    select a w' smallest element from C_2
    select arbitrary $w : w \in C_1$, where $d(w, w') = d'$
    select arbitrary index j, where $w[j] \neq w'[j]$
    denote $a := w[j], b := w'[j]$
    for each $y \in C_2$ **do**
      if $y[j] = a$ **then**
        $y[j] = b$
      else if $y[j] = b$ **then**
        $y[j] = a$
      end if
    end for
  end if
end while
STOP, OUTPUT: $C' := C_1$

PROJECT FINANCED FROM THE NRDI FUND

Development III

Contact graph (unconnected, can be improved)



Second lemma I

Proposition

Let $H \stackrel{\text{def}}{=} \mathbb{Z}_{k_s}^{\alpha_s} \times \cdots \times \mathbb{Z}_{k_2}^{\alpha_2} \times \mathbb{Z}_{k_1}^{\alpha_1}$, where $\min_i k_i \geqslant 3$ and $d \leqslant n, d \in \mathbb{N}$. Every maximal Hamming packing $C \subseteq H$ with minimal distance d can be transformed to another maximal Hamming packing C' with the same number of codewords and minimal distance, whose contact graph $CG(C')$ is connected and for every $v \in V(CG(C'))$ holds that $deg(v) \geqslant 2$.

Second lemma II

Proof

According to proposition 1, there exists a connected contact graph $G \overset{\text{def}}{=} CG(C)$. This implies that every node $v \in V(G)$ has a degree $deg(v) \geqslant 1$. Without the loss of generality assume that there is a node $z \overset{\text{def}}{=} \overline{00\ldots0}$ such that $deg(z) = 1$, and its only neighbour node is $w_0 \overset{\text{def}}{=} \overline{\underbrace{00\ldots0}_{n-d}\underbrace{11\ldots1}_{d}}$ (after permuting the member sets in the defining Cartesian product of H to simplify the notation).

Second lemma III

Proof (contd.)

Now introduce a set of codewords $w_i \overset{\text{def}}{=} \overline{\underbrace{00\ldots0}_{n-d}\underbrace{11\ldots1}_{d-i}\underbrace{22\ldots2}_{i}}$ for every $1 \leqslant i \leqslant d, i \in \mathbb{N}$. There exist such nodes because there are no binary alphabets in the decomposition of H. Now, for all i, check if w_0 can be replaced with w_i. Node w_d should be a codeword $s \in V(G) \backslash \{z, w_0\}$ such that $d(w_d, s) < d$, otherwise $C \bigcup^* \{w_d\}$ will be a feasible d-packing contradicting the maximality of $|C|$.

Second lemma IV

Proof (contd.)

Now regarding the $d+1$ members of the ordered list $(w_i)_{0\leqslant u\leqslant d}$, in each following codeword pair, there is exactly one symbol change, yielding an estimation that its Hamming distance from the set $D \stackrel{\text{def}}{=} C\setminus\{z, w_0\}$ can change by at most 1. But $d(D, w_0) > d$ and $d(D, w_d) < d$, which means that there must be at least one word $w_j : d(D, w_j) = d$. By replacing w_0 to w_j yields a packing C' with the same cardinality as C but with strictly less 1-degree node in its contact graph.
Iterating this process can be done in finitely many times due that C is finite, and the resulting modified packing has a contact graph with the necessary properties. □

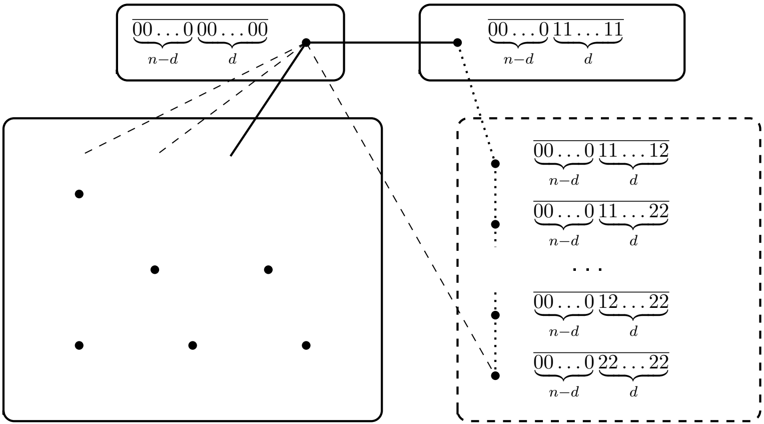
Second lemma V

Corollary

- It is worth to notice that for every maximal packing in arbitrary mixed Hamming spaces, every connected contact graph can be improved by eliminating all nodes with degree 1 if such a node and its only neighbour differs in nonbinary alphabet positions only.
- Adding constraints derived from the second lemma has a drawback: a solution vector would not necessarily be feasible if some of the 1s are replaced to 0s.

Second lemma VI

Figure sketch for 2nd lemma's proof

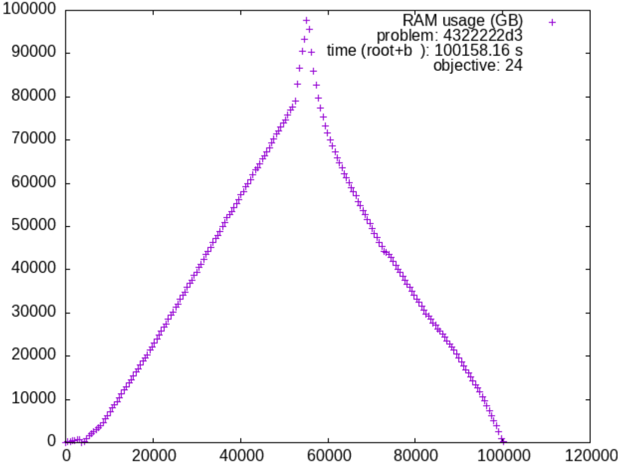


Results

4443222:3 753222:3 63322222:3 92222222:3 444222:3 543332:3 554442:3 5552222:3 4332222:3 7622222:3
833222:3 9333222:3 6322222:3 544432:3 544333:3 5332222:3 854322:3 733222:3 9422222:3 844222:3 555533:3
3333222:3 553332:3 7722222:3 83222222:3 643333:3 993222:3 533322:3 842222:3 4444442:3 543333:3 43332222:3
872222:3 833332:3 633332:3 654422:3 633333:3 843322:3 733332:3 753322:3 6542222:3 532222:3 7522222:3
7442222:3 554443:3 6333322:3 443333:3 5433222:3 744422:3 4433322:3 553333:3 955222:3 6442222:3 553322:3
953222:3 9322222:3 762222:3 663222:3 444322:3 732222:3 9522222:3 82222222:3 733333:3 544444:3 953322:3
433333:3 992222:3 6532222:3 6622222:3 763322:3 444444:3 633322:3 63222222:3 444422:3 74222222:3 933332:3
722222:3 6433222:3 772222:3 755222:3 952222:3 443222:3 444443:3 632222:3 622222:3 653332:3 744222:3
32222222:3 542222:3 444442:3 64222222:3 433332:3 644422:3 3333322:3 964222:3 9622222:3 655222:3 6522222:3
5333322:3 843222:3 8332222:3 6332222:3 552222:3 544442:3 743322:3 555422:3 844322:3 933322:3 555555:3
3333332:3 644322:3 554444:3 922222:3 5322222:3 873222:3 7532222:3 332222:3 4444222:3 743332:3 775222:3
633222:3 554432:3 933333:3 764222:3 865222:3 643322:3 963322:3 5522222:3 443332:3 333333:3 8222222:3
533222:3 852222:3 8532222:3 7322222:3 53322222:3 444433:3 7333222:3 554332:3 742222:3 4422222:3 664222:3
442222:3 7422222:3 533333:3 5533222:3 543222:3 765222:3 862222:3 544443:3 554333:3 8722222:3 3222222:3
544332:3 5222222:3 554422:3 . . .

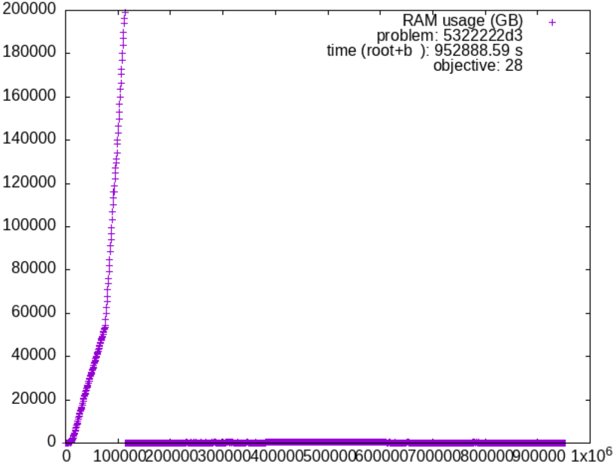
PROJECT FINANCED FROM THE NRDI FUND

Results



Best value: 24, problem is $N_{4,3,2}(1,1,5;d=3)$

Results



Best value: 28, problem is $N_{5,3,2}(1,1,5;d=3)$

Conclusions

- With the right *decomposition*, the classic solvers after formulating LP ... might compete with clique-based packing searchers
  - $N_{2,3}(7, 1; d = 3) = 26$, solved in 6 hours
  - $N_{2,3}(4, 3; d = 3) = 28$, solved in 5 days
  - record keeper is: P. Östergård, (1999, 2000)
    P. R. J. Östergård, Classification of binary/ternary one-error-correcting codes, Discrete Math. 223 (2000) 253-262.

    https://www.win.tue.nl/~aeb/codes/
- Zero mipgaps proving the optimality of the above
- RAM- and CPU-intensive models
- Reliable GPU support of MILP solvers is a challenge
- Low-hanging fruits were picked - more or less

https://arxiv.org/abs/2310.01883

PROJECT FINANCED FROM THE NRDI FUND

D-Wave

Work in progress.

Settings

system	`Advantage_system4.1`
samples	1000
tau	(annealing time / sample) $20\mu s$
others	default

Decomposition has been applied. $\mapsto$ About 100 logical qubits.

Importance of the decomposition

QUBO's as well as the problem size can be reduced when searched for feasible packings having connected contact graphs!

PROJECT FINANCED FROM THE NRDI FUND

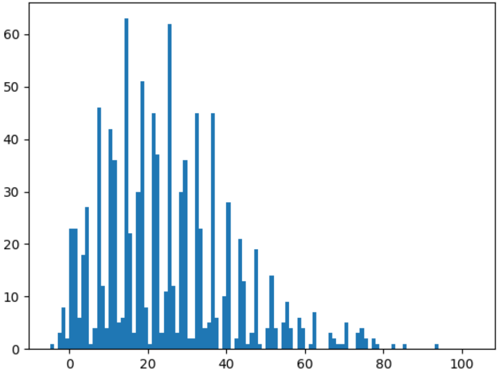
D-Wave

problem name (maximizing)	CPLEX time (ms)	CPLEX optimum	Total QPU access time	DWave optimum	No. of subproblems
$N(3^2, 2^5, d = 3)$	401730	22	4129	15	15
$N(4, 2^7, d = 4)$	1120	16	1989	10	7*
$N(4, 2^6, d = 3)$	737200	18	1810	14	7
$N(4, 3^4, d = 3)$	102510	21	3662	12	13
$N(4^2, 2^5, d = 4)$	2542180	9	3935	8	15
$N(5, 4, 2^4, d = 3)$	130	16	6337	13	23

*: 2 subproblems could not have been embedded:

$\{0, 10000111, 10011001\}$ and $\{0, 00001111, 10010011\}$

A histogram



Best value: -5, thus the result is 3 - (-5) = 8. The optimum is 9.

Conclusions so far (quantum)

- With the right *decomposition*, the quantum annealer is at least promising.
- Further tweaking is needed (annealing time, schedules, etc.).
- Best used as a subroutine.
  - $N_{2,3}(7, 1; d = 3) = 26$, trivially reduced QUBO's theoretic best optimum is 25, D-Wave hybrid solver gave 24. But is a black box...
- Such packing search models "scale" automatically according to the quantum-"Moore's law"
- As small as 300 sized yet unsolved QUBO problems exists - after size reduction

PROJECT FINANCED FROM THE NRDI FUND

Acknowledgements

- Development and Innovation Office
  within the
  Quantum Information National Laboratory of Hungary
- Wigner Scientific Computing Laboratory (WSCLAB)

wigner QNL Quantum Information National Laboratory HUNGARY

National Research, Development and Innovation Office Hungary
PROJECT FINANCED FROM THE NRDI FUND

wigner QNL Quantum Information National Laboratory HUNGARY
National Research, Development and Innovation Office Hungary
PROJECT FINANCED FROM THE NRDI FUND