

Effective Prime Factorization via Quantum Annealing by Modular Locally-structured Embedding

Jingwen Ding¹, Giuseppe Spallitta¹, and Roberto Sebastiani¹

¹University of Trento, Trento (Italy)

¹{jingwen.ding, giuseppe.spallitta, roberto.sebastiani}@unitn.it

ABSTRACT

This paper investigates novel techniques to solve prime factorization by quantum annealing (QA). Our contribution is twofold. First, we present a novel and very compact modular *encoding* of a binary multiplier circuit into the Pegasus architecture of current D-Wave QA devices. The key contribution is a compact encoding of a controlled full-adder into an 8-qubit module in the Pegasus topology, which we synthesized offline by means of Optimization Modulo Theories. This allows us to encode up to a 21×12 -bit multiplier (and a 22×8 -bit one) into the Pegasus 5760-qubit topology of current annealers. To the best of our knowledge, these are the largest factorization problems ever encoded into a quantum annealer.

Second, we have investigated the problem of actually *solving* encoded PF problems by running an extensive experimental evaluation on a D-Wave Advantage 4.1 quantum annealer. In order to help the annealer in reaching the global minimum, in the experiments we introduced different approaches to initialize the multiplier qubits and adopted several performance enhancement techniques. Overall, exploiting all the encoding and solving techniques described in this paper, $8,219,999 = 32,749 \times 251$ was the highest prime product we were able to factorize within the limits of our QPU resources. To the best of our knowledge, this is the largest number which was ever factorized by means of a quantum annealer, and, more generally, by a quantum device.

Introduction

Integer factorization (IF) is the problem of factoring a positive integer into a product of small integers, called factors. If the factors are restricted to be prime, we refer to it as prime factorization (PF). Finding the prime factors of prime numbers becomes increasingly difficult as the numbers get larger. This difficulty is exploited in modern cryptography, where prime factorization is used as a basis for secure encryption algorithms (e.g. the RSA public-key encryption¹) since the process of factoring large numbers is currently considered computationally infeasible for classical computers.

Quantum computers have the potential to perform PF exponentially faster than classical computers. A first approach in tackling PF by quantum computing is *Shor's algorithm*². This technique takes advantage of the properties of quantum mechanics, such as superposition and entanglement, to factor numbers into their prime factors in poly-logarithmic time. Although several efforts in implementing this algorithm, and variations thereof, on existing gate-based quantum computers have been presented in the literature³⁻⁷, plus other approaches⁸, the size of IP/PF which were actually implemented and solved on pure quantum devices is very small, in the order of few thousands. (Notice that a large-scale simulation of Shor's algorithm of GPU-based classical supercomputer allowed to factorize up to 549,755,813,701⁹, and that the factorization of the single number 1,099,551,473,989 was made possible by means of hybrid quantum-classical algorithms¹⁰.) *Quantum Annealing (QA)* has shown to be effective in performing prime factorization, e.g., by reducing high-degree cost functions to quadratic either by using Groebner bases¹¹ or by using equivalent quadratic models produced by adding ancillary variables¹², or by related approaches¹³. Currently, the largest factorization problem mapped to the quantum annealer D-Wave 2000Q is 376,289. Moreover, all bi-primes up to 200,000 have been solved by D-Wave 2X processors^{11, 12}. Also, by using D-Wave hybrid Classic-QA tool, 1,005,973 has been factored¹⁴. (See Willsch et al.⁹ for a recent very-detailed survey on solving PF with quantum devices.)

In this paper, we propose a novel approach based on a modular version of locally-structured embedding of satisfiability problems^{15, 16} to encode IF/PF problems into Ising models and solve them using QA. Our contribution is twofold.

First, we present a novel modular *encoding* of a binary multiplier circuit into the architecture of the most recent D-Wave QA devices. The key contribution is a compact encoding of a controlled full-adder into an 8-qubit module in the Pegasus topology¹⁷, which we synthesized offline by means of Optimization Modulo Theories. The multiplier circuit is then built by exploiting a bunch of novel ideas, namely *alternating modules*, *qubit sharing* between neighboring modules, and *virtual chaining* between non-coupled qubits. This allows us to encode up to a 21×12 -bit multiplier (resp. a 22×8 -bit one) into the Pegasus 5760-qubit topology of current annealers, so that a fault-free annealer could be fed an integer factorization problem up to $8,587,833,345 = 2,097,151 \times 4,095$ (resp. $1,069,547,265 = 4,194,303 \times 255$), allowing for prime factorization of up to $8,583,606,299 = 2,097,143 \times 4,093$ (resp. $1,052,769,551 = 4,194,301 \times 251$). To the best of our knowledge, these

are the largest factorization problems ever encoded into a quantum annealer. We stress the fact that, given the modularity of the encoding, this number scales up automatically with the growth of the qubit number in the chip.

Second, we have investigated the problem of actually *solving* encoded PF problems by running an extensive experimental evaluation on a D-Wave Advantage 4.1 quantum annealer. Due to faulty qubits and qubit couplings of the QA hardware we had access to, it was possible to feed to it at most a 17×8 -bit multiplier, corresponding to at most a $33,423,105 = 131,071 \times 255$ factorization. In order to help the annealer in reaching the global minimum, in the experiments we introduced different approaches to initialize the multiplier qubits and adopted several performance enhancement techniques, like *thermal relaxation*, *pausing*, and *reverse annealing*, which we combined together by iterative strategies, discussing their synergy when combined. Overall, exploiting all the encoding and solving techniques described in this paper, $8,219,999 = 32,749 \times 251$ was the highest prime product we were able to factorize within the limits of our QPU resources. To the best of our knowledge, this is the largest number which was ever factorized by means of a quantum annealer, and more generally by a quantum device, without adopting hybrid quantum-classical techniques.

Disclaimer. Due to space constraints, some details in some figures may not be easy to grasp from a printed version of this paper. Nevertheless, all figures are high-resolution ones, so that every detail can be grasped in full if they are seen via a pdf viewer.

Foundations

D-Wave quantum annealers

From a physicist's perspective, D-Wave's quantum annealers (QAs) are quantum devices that use quantum phenomena to reach minimum-energy states in terms of the values of their *qubits* (i.e. minimum-energy states of superconducting loops). For a these QAs, the (quantum) *Hamiltonian* $H(s)$ —which corresponds to the classical Hamiltonian that described some physical system in terms of its energies— is represented by the sum of the driver Hamiltonian H_{driver} and the classical Ising Hamiltonian H_{Ising} , where $\hat{\sigma}_{x,z}^{(i)}$ are Pauli matrices operating on a qubit q_i , s.t. h_i and $J_{i,j}$ are programmable parameters representing the qubit biases and coupling strengths:

$$H(s) \stackrel{\text{def}}{=} -\frac{A(s)}{2}H_{\text{driver}} + \frac{B(s)}{2}H_{\text{Ising}}, \quad \text{s.t. } H_{\text{driver}} \stackrel{\text{def}}{=} \sum_i \hat{\sigma}_x^{(i)}, \quad H_{\text{Ising}} \stackrel{\text{def}}{=} \sum_i h_i \hat{\sigma}_z^{(i)} + \sum_{i>j} J_{i,j} \hat{\sigma}_z^{(i)} \hat{\sigma}_z^{(j)}. \quad (1)$$

The parameter s is the normalized anneal fraction, $s = t/t_f \in [0, 1]$, where t is time and t_f is the total time of the anneal process. This s -dependent Hamiltonian $H(s)$ smoothly interpolates between H_{driver} and H_{Ising} through the two annealing functions $A(s), B(s)$, as shown in Figure 1a. At $s = 0$, the system starts in the groundstate of H_{driver} , with all qubits in the superposition state of 0 and 1; as the system is annealed $s \uparrow$, the dominance of H_{driver} decreases and H_{Ising} comes to play; at the end of the annealing process $s = 1$, the system would end up in a classical state that corresponds to H_{Ising} . According to the quantum adiabatic theorem, the system will remain in the instantaneous groundstate through the evolution iff the system is annealed slowly enough. The required runtime according to the theorem is proportional to $\frac{1}{\text{gap}^2}$, where gap is the minimal gap between the ground state and excited states during the system evolution.

From a computer scientist's perspective, D-Wave's QAs are specialized quantum computers which draw optima or near-optima from quadratic cost functions on binary variables, that is, specialized hardware for solving the *Ising problem*:¹⁶

$$\underset{\underline{z} \in \{-1, 1\}^{|V|}}{\text{argmin}} H(\underline{z}), \quad \text{s.t. } H(\underline{z}) \stackrel{\text{def}}{=} \sum_{i \in V} h_i z_i + \sum_{(i,j) \in E} J_{i,j} z_i z_j, \quad (2)$$

where each variable $z_i \in \{-1, 1\}$ is associated with a qubit; $G = \langle V, E \rangle$ is an undirected graph, the *hardware graph* or *topology*, whose edges correspond to the physically-allowed qubit interactions; and $h_i, J_{i,j}$ are programmable real-valued parameters. The current Pegasus topology¹⁷ was introduced in the D-Wave Advantage quantum annealing machine and is based on a lattice of qubits. The lattice is divided into cells (“tiles”), where each cell contains eight qubits arranged in a bipartite graph. We call qubits on the same side of the partition either *vertical* or *horizontal* qubits. Qubits of the same side inside each tile are connected 2-by-2. Figure 1b shows the Pegasus topology for a 3×3 subgraph. It extends the previous Chimera topology by adding more connections between the tiles so that the degree of connectivity of each qubit is up to 15. In particular, each tile is now connected to diagonally neighboring tiles through 45° , 120° and 150° connections among qubits w.r.t. the x axis (we will refer to them as *diagonal couplings*). Moreover, the configurable range of coefficients also increases, e.g., D-Wave Advantage 4.1 systems allow for biases and couplings s.t. $h_i \in [-4, 4]$ and $J_{i,j} \in [-2, 1]$.

Monolithic encoding of small SAT problems based on OMT

Bian et al.¹⁶ formulated the problem of encoding SAT problems into *Ising models* that are compatible with the available quantum topology —represented as a graph (V, E) s.t. the nodes V are the qubits and the edges E are the qubit couplings—with the goal of feeding them to the quantum annealer. Here we briefly summarize their techniques, adopting the same notation.

Given a (small enough) Boolean formula $F(\underline{x})$ and a set of extra Boolean variables \underline{a} (called *ancillae*), we first need to map the Boolean variables \underline{x} and \underline{a} into a subset $\underline{z} \subseteq V$ of the qubits in the topology, with the intended meaning that the qubit values

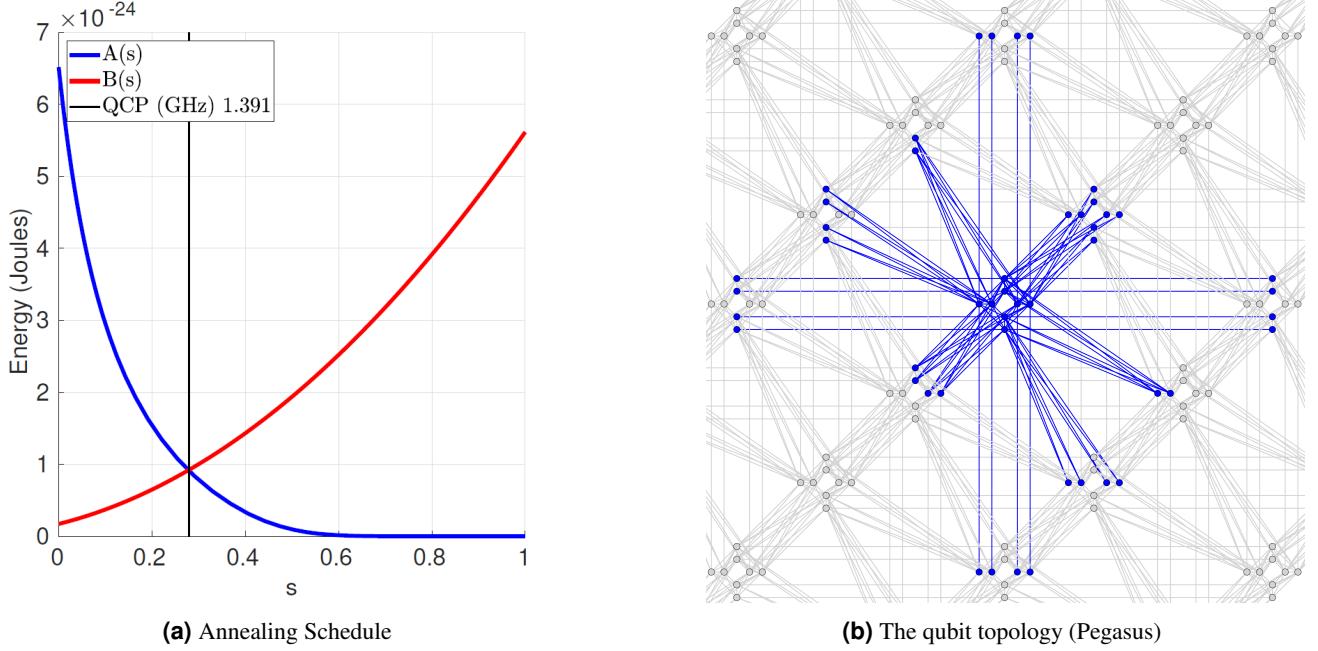


Figure 1. Information about the D-Wave Pegasus systems and their behavior.

$\{1, -1\}$ are interpreted as the truth values $\{\top, \perp\}$ respectively. (With a little abuse of notation, we consider this map implicit and say that $\underline{z} \stackrel{\text{def}}{=} \underline{x} \cup \underline{a}$.) This map, called *placement*, can be performed either manually or via ad-hoc procedures¹⁶.

Then we need to compute the values θ_0 , θ_i , and θ_{ij} of a *penalty function* $P_F(\underline{x}, \underline{a} | \theta)$ such that, for some value $g_{min} > 0$:

$$P_F(\underbrace{\underline{x}, \underline{a}}_{\underline{z}} | \theta) \stackrel{\text{def}}{=} \theta_0 + \sum_{z_i \in V} \theta_i z_i + \sum_{(z_i, z_j) \in E, i < j} \theta_{ij} z_i z_j; \quad z_i \in \{-1, 1\}; \quad \forall \underline{x} \min_{\{\underline{a}\}} P_F(\underline{x}, \underline{a} | \theta) \begin{cases} = 0 & \text{if } F(\underline{x}) = \top \\ \geq g_{min} & \text{if } F(\underline{x}) = \perp \end{cases} \quad (3)$$

Intuitively, $P_F(\underline{x}, \underline{a} | \theta)$ allows for discriminating truth values for \underline{x} which satisfy the original formula $F(\underline{x})$ (i.e., these s.t. $\min_{\{\underline{a}\}} P_F(\underline{x}, \underline{a} | \theta) = 0$) from those who do not (i.e., these s.t. $\min_{\{\underline{a}\}} P_F(\underline{x}, \underline{a} | \theta) \geq g_{min}$). θ_0 , θ_i , θ_{ij} and g_{min} are called respectively *offset*, *biases*, *couplings* and the *gap*; the offset has no bounds, whereas biases and couplings have a fixed range of possible values ($[-2, +2]$ for biases and $[-1, +1]$ for coupling for the old Chimera architecture, $[-4, +4]$ for biases and $[-2, +1]$ for couplings for the Pegasus architecture of Advantage systems).

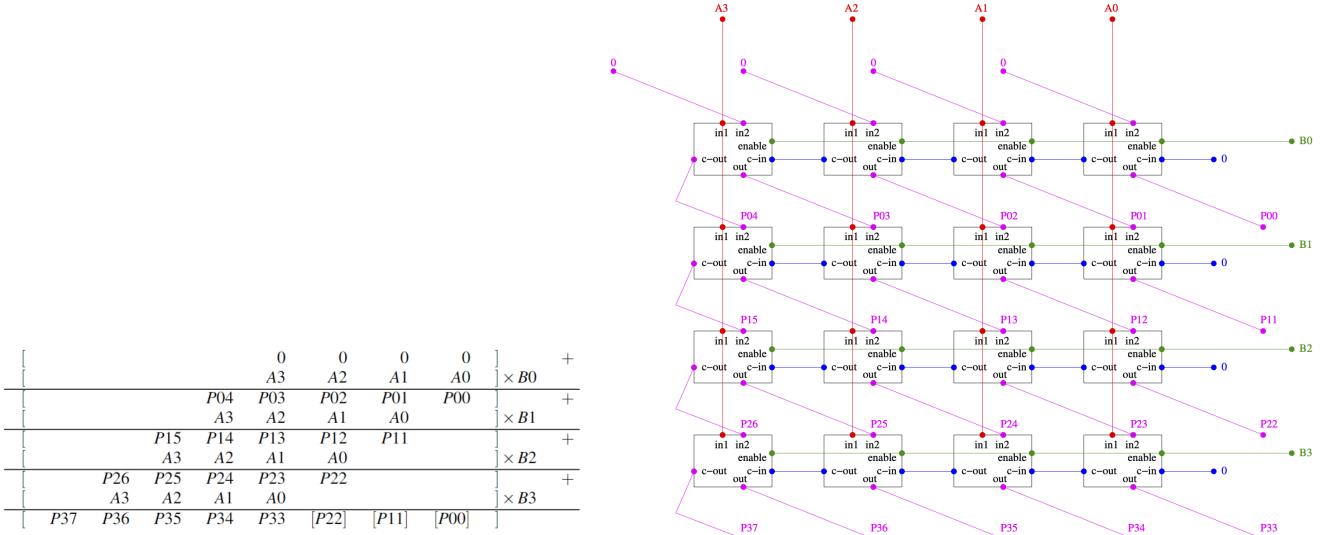
The penalty function $P_F(\underline{x}, \underline{a} | \theta)$ (3) is fed to the quantum annealer, which tries to find values for the \underline{z} 's which minimizes it. Once the annealer reaches a final configuration, if the corresponding energy is zero, then we can conclude that the original formula is satisfiable and the values of $\underline{x} \subseteq \underline{z}$ satisfy $F(\underline{x})$ —once reconverted from $\{1, -1\}$ to $\{\top, \perp\}$. Notice that we may have a solution for $F(\underline{x})$ even if the energy of the assignment is not zero, because the truth values of the ancillae do not impact the satisfiability of the original formula $F(\underline{x})$ but may affect the final energy. (We will call them “ > 0 -energy solutions”.) This is not an issue, because checking if the truth assignments of the variables in \underline{x} satisfy $F(\underline{x})$ is trivial. Notice also that, since the annealer is not guaranteed to find a minimum, if the result is not a solution, then we cannot conclude that $F(\underline{x})$ is unsatisfiable.

The gap g_{min} between ground and non-ground states has a fundamental role in making the annealing process more effective: the bigger g_{min} , the easier is for the annealer to discriminate between satisfying and non-satisfying assignments. Ancillae \underline{a} are needed to increase the number of θ parameters, because the problem of finding a suitable $P_F(\underline{x}, \underline{a} | \theta)$ matching (3) is over-constrained in general, so that without ancillae there would be no penalty function even for very few variables \underline{x} 's (e.g., > 3). The more ancillae, the more degrees of freedom, the higher the chances to have a suitable penalty with a higher gap g_{min} .

The problem of synthesizing $P_F(\underline{x}, \underline{a} | \theta)$ is solved by using a solver for *Optimization Modulo Theories* such as OptiMathSAT¹⁸. For the Pegasus architecture, we feed OptiMathSAT some formula equivalent to:

$$\forall \underline{x}. \left[\begin{array}{l} (F(\underline{x}) \rightarrow \exists \underline{a}. (P_F(\underline{x}, \underline{a} | \theta) = 0)) \wedge \\ (F(\underline{x}) \rightarrow \forall \underline{a}. (P_F(\underline{x}, \underline{a} | \theta) \geq 0)) \wedge \\ (\neg F(\underline{x}) \rightarrow \forall \underline{a}. (P_F(\underline{x}, \underline{a} | \theta) \geq g_{min})) \wedge \\ \bigwedge_i (\theta_i \in [-4, 4]) \wedge \bigwedge_{i,j} (\theta_{ij} \in [-2, 1]) \end{array} \right], \quad (4)$$

asking to find the set of values of the θ s satisfying (4) which maximizes the gap g_{min} . The result, if any, is a suitable $P_F(\underline{x}, \underline{a} | \theta)$.



(a) The theoretical idea behind a 4×4 -bit shift-and-add multiplication

(b) The 4×4 -bit multiplier schema of Figure 2a

Figure 2. Details about the modularity of shift-and-add multipliers.

Locally-structured embedding for large SAT problem

Encoding a Boolean formula $F(\underline{x})$ using the monolithic encoding shown in (4) presents several limitations. In practice, no more than 10 qubits can be considered if we directly use the formulation in equation (4), and recalling that some of them are required as ancillary variables, the set of Boolean formulas we can encode monolithically this way is quite limited.

To encode larger propositional problems, Bian et al.¹⁶ proposed a *divide-and-conquer* strategy. The original formula is first And-decomposed into smaller sub-formulae so that the penalty function $P_F(\underline{x}, \underline{a}|\theta)$ for each subformula can be computed for some given placement. In particular, given a formula $F(\underline{x})$, we can And-decompose it as $F(\underline{x}) := \bigwedge_{k=1}^K F_k(\underline{x}^k)$, s.t. each penalty function can be computed offline by OptiMathSAT. The *And-decomposition property*¹⁶ guarantees under some conditions that the penalty function of the original formula $F(\underline{x})$ can be easily obtained by summing up all the penalty functions from the subformulae: $P_F(\underline{x}, \underline{a}|\theta) = \sum_k P_{F_k}(\underline{x}^k, \underline{a}^k|\theta^k)$, where $g_{\min}(F(\underline{x})) = \min_k(g_{\min}(F_k(\underline{x})))$. The penalty function $P_{F_k}(\underline{x}^k, \underline{a}^k|\theta^k)$ of each sub-formula $F_k(\underline{x}^k)$ is then mapped into a subgraph in the QA topology –e.g. one of the tiles in the Pegasus topology.

When two sub-formulae $F_i(\underline{x}^i)$ and $F_j(\underline{x}^j)$ share one (or more) Boolean variables x , we can (implicitly) rename one of the two occurrences into x' and conjoin a chain of equivalences $x \leftrightarrow \dots \leftrightarrow x'$ to them. (I.e., $F_i(\dots, x, \dots) \wedge F_j(\dots, x, \dots)$ can be (implicitly) rewritten into $F_i(\dots, x, \dots) \wedge F_j(\dots, x', \dots) \wedge (x \leftrightarrow \dots \leftrightarrow x')$.) This corresponds to linking the corresponding qubits x and x' in the penalty functions $P_{F_i}(\underline{x}^i, \underline{a}^i|\theta^i)$ and $P_{F_j}(\underline{x}^j, \underline{a}^j|\theta^j)$ by means of a *chain* of unused qubits used as ancillary variables, forcing all involved qubits to assume the same truth value, by using the *equivalence chain penalty function* $\sum_{(z, z') \in \text{chain}} (2 - 2zz')$ for the qubits in the chain, corresponding to the Boolean formula $x \leftrightarrow \dots \leftrightarrow x'$ (here we consider the Pegasus extended ranges). The final penalty function is the sum of the penalty functions from the decomposition phase with those of the chains.

We refer the reader to Bian et al.¹⁶ for a more detailed description of these techniques.

Encoding binary multipliers into Pegasus quantum annealers

Modular representation of a multiplier

In a fashion similar to Bian et al.¹⁶, we developed a *modular* encoding of a shift-and-add multiplier, so that it could be easily extended for future larger quantum devices. To this extent, the binary-arithmetic computation of multiplications, as shown in Figure 2a, is based on a module implementing a *Controlled Full-adder* (CFA). The Boolean representation of a single CFA is:

$$\begin{aligned} CFA(in2, in1, enable, c_in, c_out, out) &\stackrel{\text{def}}{=} (c_out \leftrightarrow ((c_in \wedge ((enable \wedge in1) \vee in2)) \vee ((enable \wedge in1) \wedge in2)) \\ &\quad \wedge (out \leftrightarrow ((enable \wedge in1) \oplus in2 \oplus c_in)) \end{aligned}$$

The structure of a CFA includes four inputs: two operand bits ($in1$ and $in2$), a control bit ($enable$) and a carry-in bit c_in . The output-carry bit c_out and the output out of a CFA are computed as is typically done for classical full adder, the only

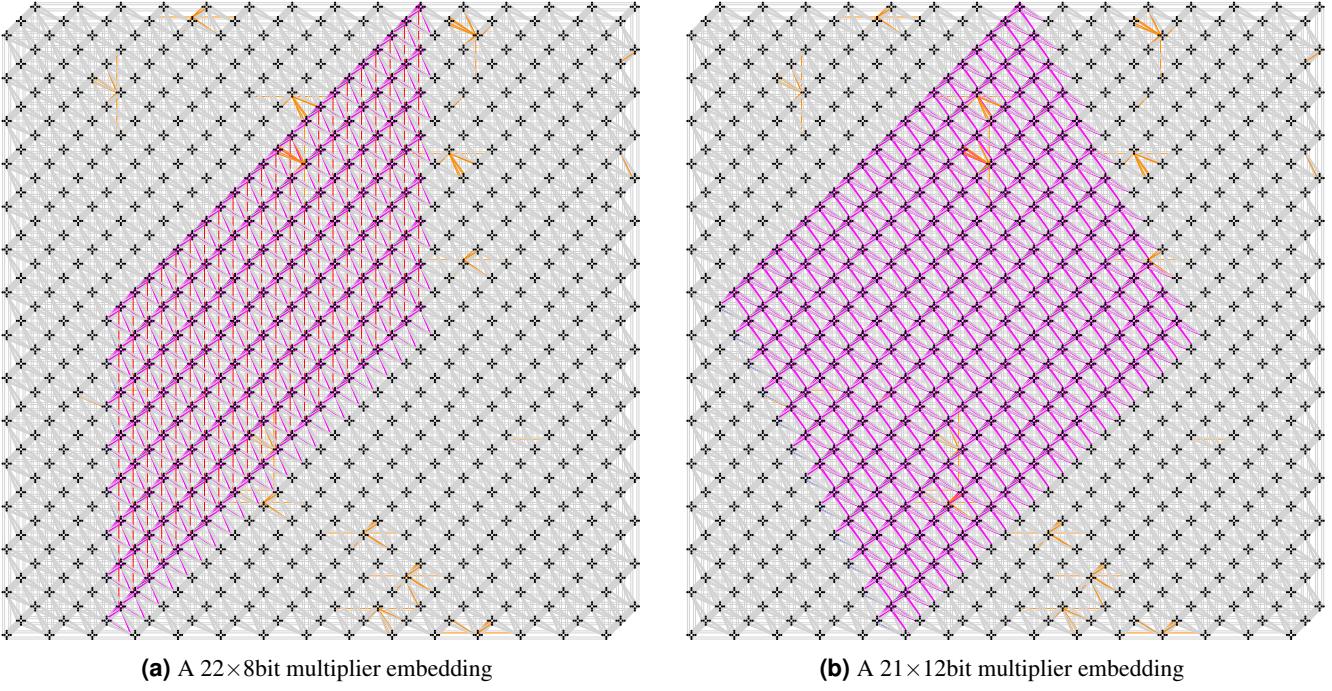


Figure 3. Modular encoding of binary multipliers on the D-Wave Pegasus topology.

difference being the the fact that the input *in1* is enabled by the *enable* bit: when *enable* is true, the CFA behaves as a standard full adder; when *enable* is false, the CFA behaves as if *in1* were false.

As shown in Figure 2b, an $m \times n$ -bit multiplier can be encoded using $m \cdot n$ CFAs as follows:

$$F_{P=A \times B} = \bigwedge_{i=0}^{n-1} \bigwedge_{j=0}^{m-1} CFA(in2^{(i,j)}, in1^{(i,j)}, enable^{(i,j)}, c_in^{(i,j)}, c_out^{(i,j)}, out^{(i,j)}) \wedge \bigwedge_{(x,x') \in chains} (x \leftrightarrow x') \quad (5)$$

where *chains* corresponds to the set of all the equivalence chains corresponding to the links between bits belonging to different CFAs, as in Figure 2b (e.g. $(enable^{(i,j)} \leftrightarrow enable^{(i,j+1)})$).

LSE-based encoding with qubit sharing, virtual chains, and alternating CFAs

A direct approach to building multipliers using multiple CFAs is to encode each CFA into a single Pegasus tile, using 2 of the 8 total qubits as ancillae. Once the penalty function for a single CFA has been obtained, we can embed them modularly and generate a grid of CFAs that simulates the multiplier. Since some qubits are shared among different CFAs, we must add equivalence chains to force the equality of the values of the corresponding qubits. First, the carry-out *c_out* qubit of a CFA placed into one tile must be linked to the carry-in *c_in* qubit of the CFA placed in the tile hosting the left CFA in the grid in Figure 2b. The same applies to the output *out* of a CFA and the input *in2* in the bottom-left CFA in Figure 2b. Lastly, it is necessary to generate the qubits links corresponding to the long red vertical chain and the green horizontal chain in Figure 2b, linking respectively the *in1* and *enable* bits.

In the Pegasus topology, each tile has some direct connections with the neighbor tiles along several directions (expressed in degrees counterclockwise wrt. the horizontal line): 0° , 90° , 45° , 120° and 150° . Considering all these constraints, two macro-configurations for placing the CFA grid of Figure 2b into a Pegasus architecture can be considered. In both configurations, due to the high number of inter-tile 45° connections, the horizontal connections in Figure 2b (the *c_out* – *c_in* and *enable* links) are placed along the 45° inter-tile connections. With the first configuration, in Figure 3a, the input qubits *in1* from vertically aligned CFAs in the grid are connected by 90° inter-tile connections and the *out* – *in2* links are connected via 120° ones. This allows for fitting a 22×8 -bit multiplier into the whole Pegasus topology. The second configuration, in Figure 3b, differs from the first one by chaining the *in1* qubits along 120° connections and the *out* – *in2* links along 150° ones. Using diagonal chains has the main advantage to fit a larger 21×12 -bit multiplier. Both configurations work modulo symmetries: for instance, encoding the grid of CFAs such that the input variable *in1* is propagated bottom-up instead of top-down is feasible by slightly changing the qubits placement into the tile.

Unfortunately, an 8-qubit CFA encoding to replicate the two configurations described above turned out to be unfeasible in practice, because no such encodings can be generated. This fact is due to two main issues: (i) the low number of ancillae

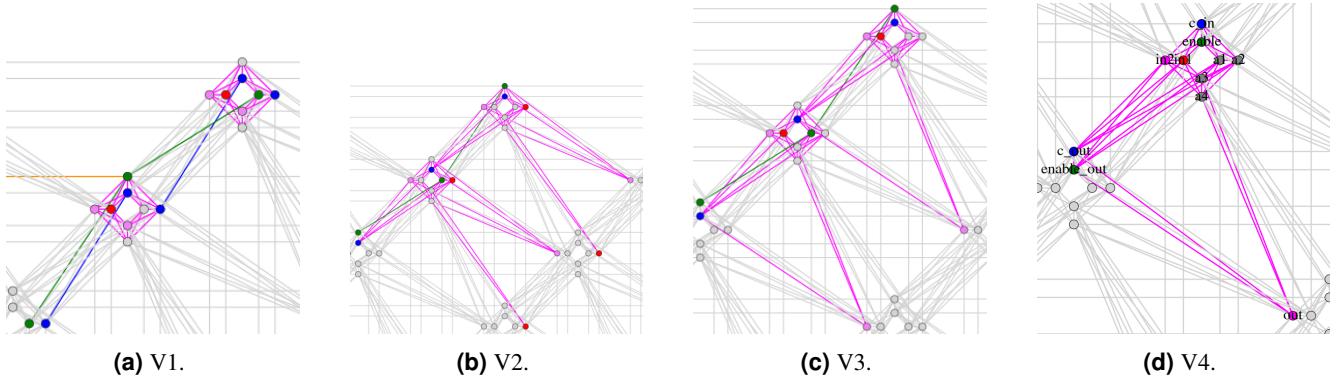


Figure 4. CFA structure for the four versions of multipliers.

(only 2) available for encoding each CFA, which drastically reduces the chances of finding a suitable penalty function, and (ii) the absence of pairwise direct 45° couplings between the same qubits in the neighbor tiles, which prevents any direct implementation of the *enable* chain along the 45° direction. (A similar issue occurs also in the second macro-configuration of Figure 3b for the *in1* bit along the 120° direction.)

To cope with these issues, we propose three novel techniques: *Alternating CFAs*, *Qubit sharing*, and *Virtual chaining*.

Alternating CFAs. To address the issue (ii) of missing couplings between qubits on the 45° direction, we propose to alternate two slightly-different CFAs in tiles along the 45° line. In particular, in Figure 4b and 4c we make the OMT solver compute two different CFAS forcing *enable* to be positioned respectively in the first vertical qubit on the upper tile and the third horizontal qubit in the 45° -degree bottom-left tile. Such qubits are pairwise directly coupled, allowing thus a chain for *enable* qubit along the 45° -degree direction (the green links). We stress the fact that the two different CFA encodings are not guaranteed to have the same gap g_{min} , and that different placements leading to different g_{min} values typically may negatively affect the annealing process.

Qubit sharing. To address the issue (i) of the low number of ancillae, we propose a technique to *share qubits between neighboring tiles*. Rather than connecting two qubits from different CFAs with an equivalence chain, we suggest utilizing a single qubit that is *shared* between the two CFAs. This means that the qubit will be used for the encoding of one CFA as an output variable and as an input variable for the subsequent CFA. This approach leads to partially-overlapping CFAs and the extra qubit can be used as an ancillary variable to increase the minimum gap of each CFA. Consider the schema in Figure 4d. The encoding of each CFA involves not only the 8 qubits of its tile but also the 3 qubits of neighbor tiles. In particular, the carry-out *c_out* is placed on the same qubit as the carry-in *c_in* of the next 45° -degree bottom-left tile –corresponding to the left CFA in Figure 2b– and the *out* qubit is placed in the same qubit of the *in2* of the next bottom-right 120° -degree tile –corresponding to the lower-right CFA in Figure 2b. The same idea applies also to the schemata in Figures 4b and 4c. (The role of the *enable_out* qubit in Figure 4d will be explained later.)

Notice that, since the global penalty function is the sum of the penalty functions of all CFAs plus these of all the equivalence chains, the value of the bias for the shared qubit in the global penalty function is the sum of these two qubits with different roles in the two penalty functions of the two sharing CFAs. (E.g., the bias of the qubit which is a *c_out* for one CFA and a *c_in* for another CFA is the sum of the *c_in* and *c_out* biases of a CFA encodings.) Thus, to generate penalty functions for the CFAs that allow qubit sharing, we introduce additional constraints to the OMT formulation in (4). In particular, we add an arithmetical constraint to force the sum of the biases of the shared qubits from two CFAs to fit in the bias range, thus simulating their over-imposition (e.g., we add a constraint like $(\theta_{c_in} + \theta_{c_out}) \in [-4, 4]$). In fact, if the final bias values did not fit into the range, then the D-Wave encoders would automatically rescale all values of biases and couplings, reducing the g_{min} value and thus negatively affecting the probability of reaching a global minimum.

Virtual chaining. The concept of qubit sharing can be exploited to simulate the existence of equivalence links when physical connections are missing, providing another solution to issue (ii). Consider the CFA encoding in Figure 4d and the *enable* logical variable. Its truth value is shared by all CFAs belonging to the same row in the grid so that all the *enable* qubit of each CFA should be connected by an equivalence chain with the *enable* qubit of the 45° bottom-left CFA. Unfortunately, there is no arc linking pairwise the respective qubits of the tiles along this direction.

In such cases, two qubits that are intended to hold the same truth value but lack a direct coupling can be *virtually chained* by using the links with the common neighbors. This is performed by extending the encoding as follows:

Multiplier version	V1	V2	V3	V4
Multiplier Max. Size	22×8	21×12	22×8	22×8
# of ancillae per CFA	2	4	4	4
# of different CFA encodings	2	2	2	1
Gap of CFA penalty functions	$(1, \frac{4}{9})$	$(2, \frac{4}{3})$	(2,2)	2
Connection $in1(i, j) - in1(i+1, j-1)$	Chain (90°)	Virtual chain (120°)	Chain (90°)	Chain (90°)
Connection $enable(i, j) - enable(i, +1)$	Chain (45°)	Chain (45°)	Chain (45°)	Virtual chain (45°)
Connection $c_in(i, j) - c_out(i, j+1)$	Chain (45°)	Qubit sharing	Qubit sharing	Qubit sharing
Connection $out(i, j) - in2(i+1, j-1)$	Chain (45°)	Qubit sharing	Qubit sharing	Qubit sharing

Table 1. Comparison of the four multipliers obtained through qubit sharing and virtual chaining.

- (a) create a new virtual logical variable (i.e. $enable_out$) to be placed in the qubit in the neighbor tile corresponding to the variable we want to chain virtually (i.e. $enable$);
- (b) extend the formula defining a CFA by conjoining the equivalence constraint between the chained and the virtual variables (i.e., $CFA'(in2, in1, enable, c_in, c_out, out, enable_out) \stackrel{\text{def}}{=} CFA(in2, in1, enable, c_in, c_out, out) \wedge (enable \leftrightarrow enable_out)$);
- (c) build the penalty function of CFA' instead of CFA by applying qubit-sharing also to $enable$ and $enable_out$.

It should be noted that if two directly-connected qubits are both involved in qubit sharing (i.e. c_in and $enable$), then also the respective coupling is shared by the two CFAs. Therefore an arithmetic constraint must be added to force the sum of the two couplings to be in the coupling range (i.e. $(\theta_{c_in, enable} + \theta_{c_out, enable_out}) \in [-2, 1]$)).

Comparing different multiplier configurations. Overall, exploiting Alternating CFAs, qubit sharing, and Virtual chaining made it possible for us to generate four multiplier configurations, which are summarized in Table 1. Versions V1, V3 and V4 allow for implementing the 22×8 -bit schema of Figure 3a, whereas version V2 allows for implementing the 21×12 -bit schema of Figure 3b. Versions V2, V3 and V4 correspond to the encodings in Figures 4b, 4c and 4d respectively.

In particular: by exploiting *Alternating CFAs*, with versions V1, V2 and V3 (Figures 4a, 4b, 4c), we could implement an *enable* chain along the 45° diagonal, and with version V1 (Figure 4b) an *in1* chain along the 120° diagonal; by exploiting *Qubit sharing*, with versions V2, V3, V4 (Figures 4b, 4c and 4d), we have saved two qubits, which we could use as ancillae, improving also the quality of the encodings and their gap g_{min} ; by exploiting *Virtual chaining*, with V4 (Figure 4d), we could implement a virtual chain for the *enable* qubit along the 45° diagonal; with V2 (Figure 4b) we could implement a virtual chain for the *in1* qubit along the 120° diagonal.

Version V1 (Figure 4a) implements the 22×8 -bit macro-configuration of Figure 3a and relies exclusively on alternating CFAs, linking inter-tile qubits only by physical chains. Although alternation allowed the production of an actual encoding, which was not possible otherwise, without qubit sharing only two ancillae were available, producing two alternating configurations with different and very low gaps: 1 and $\frac{4}{9}$. These numbers are way lower than the gap used for chains, the annealers tend to be stuck on local minima since changing the spin of chained qubits becomes difficult.

Version V2 (Figure 4b) implements the 21×12 -bit macro-configuration of Figure 3b with alternating CFA encodings, using a virtual chain for implementing the *in1* chain along the 120° direction, and qubit sharing for the *c_in - c_out* (the blue qubits) and *out - in2* (the magenta qubits) connections, which saves two qubits and allows for 4 ancillae. This allows us to improve significantly the gaps to 2 and $\frac{4}{3}$ respectively. Nevertheless, the two CFAs have different g_{min} , which negatively affects the global gap (which is thus $\frac{4}{3}$) and thus the overall performances of the annealer.

Version V3 (Figure 4c) instead implements the 22×8 -bit macro-configuration of Figure 3a with alternating CFA encodings, using a physical 90° *in1*, also using qubit sharing for the *c_in - c_out* and *out - in2* connections, allowing 4 ancillae. With this configuration, we obtain two CFAs with identical gap 2, which is a significant improvement. Nevertheless, having two physical chains for two different variables (*enable* and *in1*) affects the annealer's performances: the longer the chains, the more difficult is for the quantum system to flip all values of the chained qubits and escape a minimum.

Version V4 (Figure 4d) also implements the 22×8 -bit macro-configuration of Figure 3a, but uses only one CFA encoding of gap 2. This is achieved by exploiting not only qubit sharing for the *c_in - c_out* and *out - in2* connections, but also virtual chaining for implementing the *enable* chain, whereas *in1* is physically chained vertically. By using a single CFA and having only one physical chain rather than two, most of the issues affecting annealing in the previous cases is solved, thus the optimization of the penalty function by the QA turns out to be more effective. Consequently, all experiments in the subsequent section employ version V4.

Solving Prime Factorization on D-Wave Advantage 4.1 system

The results presented in the previous section do not account for the actual limitations of quantum annealers. In particular, due to hardware faults, some of the qubits, and some connections between them are inactive and cannot be tuned during annealing. These inactive nodes and connections, referred to in the literature as *faulty qubits* and *faulty couplings* respectively, are spread all around the entire architecture, and are marked in orange in Figures 3a and 3b for the D-Wave Advantage 4.1 annealer, which we have used in all our experiments in this paper. Therefore, although it is theoretically possible to create multipliers up to 21×12 bits or 22×8 bits, these hardware constraints compel us to test smaller multipliers to avoid faulty qubits and couplings. An empirical evaluation of possible placements of multipliers into the Advantage 4.1 system leads us to determine an area of the architecture with no faulty nodes nor couplings that is suitable for being tested, capable of embedding a multiplier of maximum size 17×8 bits with the configuration of Figures 3a and 4d. All the experiments in this section will consider these hardware limitations. Also, the experimental evaluation reported in this section was constrained by the limited amount of QPU time on the Advantage 4.1 annealer we were given access to (600 seconds per month).

Initializing qubits

To factor a specific integer, it is necessary to initialize several qubits within the multiplier embedding: all qubits associated with the output bits need to be initialized to represent the target number for factorization —e.g., if the output $[P37\dots P00]$ of the 4×4 -bit multiplier in Figures 2a and 2b is forced to 00100011 (i.e. 35), then the corresponding qubits are initialized respectively to $\{-1, -1, 1, -1, -1, -1, 1, 1\}$; additionally, the variables c_in and $in2$ on the most external CFAs should be forced to be 0, as depicted in Figure 2b, so that their corresponding qubits should be initialized to -1 .

D-Wave Advantage interface provides an API, the `fix_variables()` function, which allows us to impose desired values on the qubits of the underlying architecture. This function operates by substituting the values of the qubits into the penalty function and subsequently rescaling the resulting penalty function to ensure all coefficients fall within the limited ranges of biases and couplings, possibly resulting into a lower g_{min} . For instance, if we have the penalty function $P_F(\underline{x}|\theta) = 2 + 4x_1 + x_2 + x_1x_2$ and we set x_2 to 1, then the penalty function becomes $P'_F(\underline{x}|\theta) = 2 + 4x_1 + 1 + x_1 = 3 + 5x_1$, which is then rescaled into $12/5 + 4x_1$ by multiplying it by a $4/5$ factor in order to fit the bias of x_1 into the $[-4, 4]$ range, thus reducing g_{min} by multiplying it the same $4/5$ factor. On the one hand, this substitution simplifies the penalty function by removing one binary variable; on the other hand, it can hurt the minimal gap due to coefficient rescaling.

To cope with the latter problem, we propose an alternative method to initialize qubits on a quantum device. We can partially influence the quantum annealer to set a specific truth value for a qubit by configuring *flux biases*¹⁹. In particular, if we want to impose the value $s_i \in \{-1, 1\}$ on a qubit, we set the flux bias for that qubit as $\phi_i = 1000\phi_0 s_i$, where ϕ_0 is the default annealing flux-bias unit of the DWave system 4.1, whereas 1000 is an empirical value we choose based on our experience.

The experiments suggested a further minor improvement in the CFA encoding. Since there may be more than one penalty function with the optimum value of g_{min} , we make a second call to an OMT solver in which we fix g_{min} and ask the solver to find a solution which also minimizes the number of those falsifying assignments which make the penalty function equal to g_{min} . The intuition here is to minimize the possibility of the annealer to get excited from ground states to first excited un-satisfying states. (Hereafter we refer as “CFA1” the CFA encoding obtained with this improvement and as “CFA0” the basic one.)

In Table 2a we compare the performances of the two initialization techniques on small prime factorization problems, with the annealing time T_a set to $10\mu s$. The column labeled $\#(P_F = 0)$ reports how many occurrences of 0-energy samples are obtained out of 1000 samples. We noticed that flux biases (with CFA1) outperform the native API, having a higher probability of reaching the global minimum. All the experiments from now on assume qubit initialization is done by tuning flux biases.

Exploiting thermal relaxation

In order to test the limits of the flux-bias initialization, we applied it to factoring the 10 largest numbers of 7×7 and 8×8 bits with the same annealing time as the previous experiments ($T_a = 10\mu s$) The results, reported in Table 2b, suggest that the success probability of getting a solution for 16-bit numbers is almost null. Increasing the annealing time T_a , however, would probably not significantly increase the success probability; to further improve the solving performances, we investigate the effectiveness of *thermal relaxation*²⁰ on solving our problems. This technique is integrated into the DWave system by introducing a *pause* T_p at a specific point S_p during the annealing process, with $S_p \in [0, 1]$. We tested it to solve 8×8 , 9×8 and 10×8 -bit factorization problems.

In the experiments, the pausing time T_p was set to $100\mu s$, whereas the pause point S_p is selected in the set $\{0.33, 0.34, \dots, 0.51\}$ and tested in ascending order until the ground state is found. The results illustrated in Table 3a, if compared with these in Table 2b, indicate the positive impact of thermal relaxation. Ground states were successfully reached for some 18-bit numbers (the largest being 256271), although challenges persist with most numbers of that size.

Size	Input N	CFA0		CFA1	
		#($P_F = 0$)	#($P_F \neq 0$)	#($P_F = 0$)	#($P_F \neq 0$)
3×3	25 (5×5)	161		136	
	35 (5×7)		389	951	
	49 (7×7)		450	997	
4×4	121 (11×11)	17		0	
	143 (11×13)		40	67	
	169 (13×13)	31		5	
5×5	289 (17×17)	5		0	
	323 (17×19)	2		0	
	361 (19×19)	1		3	
	391 (17×23)	6		9	
	437 (19×23)	17		0	
	493 (17×29)	3		2	
	527 (17×31)	21		37	
	529 (23×23)	5		8	
	551 (19×29)	0		4	
	589 (19×31)	16		52	
	667 (23×29)	0		105	
	713 (23×31)	11		138	
	841 (29×29)	5		7	
	899 (29×31)	17		343	
	961 (31×31)	1		338	

Size	Input N	#($P_F = 0$)		Size	Input N	#($P_F = 0$)	
		1	2			1	2
7×7	10,033 (127×79)	0		8×8	49,447 (251×197)	0	
	10,541 (127×83)	1			49,949 (251×199)	0	
	11,303 (127×89)	0			52,961 (251×211)	0	
	12,319 (127×97)	0			55,973 (251×223)	0	
	12,827 (127×101)	1			56,977 (251×227)	0	
	13,081 (127×103)	2			57,479 (251×229)	0	
	13,589 (127×107)	10			58,483 (251×233)	0	
	13,843 (127×109)	0			59,989 (251×239)	2	
	14,351 (127×113)	0			60,491 (251×241)	0	
	16,129 (127×127)	7			63,001 (251×251)	0	

(a) Comparison of the two initialization techniques on prime factorization of small numbers, with $T_a = 10\mu s$.

(b) Prime factorization of the 10 biggest 7×7 and 8×8 numbers configuring flux biases, with $T_a = 10\mu s$.

Table 2. Results of standard forward annealing to solve prime factorization.

Exploiting quantum local search

For the factorization problems in Table 3a that did not end up in the global minimum, we further exploited *quantum local search*, consisting of refining a sub-optimal state to reach the global minimum. Quantum local search is implemented in the DWave system by mean of *reverse annealing* (RV)²¹. The annealer is initialized in a local minimum, whereas the annealing process starts from $s = 1$ moving towards $s' = 0$ and then returning back to $s = 1$. We remark that reverse annealing admits pauses during the process: in this case, the system pauses for T_p microseconds at a middle point $s' = S'_p$.

In our experiments, we chose the lowest-energy state from table 3a as the initial state of RV. If multiple lowest-energy samples are obtained with different S_p values, we pick the one whose pause is performed later. The pause points for RV were tested in decreasing order (in opposition to forward annealing when we opted for the ascending order) until a ground state was found. The results are reported in Table 3b. We observe that reverse annealing, enhanced by thermal relaxation, helps in solving up to 9×8 -bit factorization problems. We also reported the Hamming distance ΔHAM between the lowest-energy state from forward and reverse annealing, showing how much a sample moved from one minimum to another, possibly a ground state.

For the instances that still failed to reach a solution, we investigated the impact of different pause lengths for RV to find ground states. The main observation from this additional analysis is that, given a low-energy initial state: (i) increasing the pause length and performing the pause at a late annealing point can help reverse annealing in jumping larger Hamming distances; (ii) increasing the pause length and triggering the pause at early annealing points cannot make RV move even farther. From these observations, we could imply that if the initial state of a reverse annealing process is very far from the ground state, it could be hard to reach the global minimum by only increasing the pause length. However, the local minimum used for the initial state of RV, which is obtained by standard annealing, tends to be highly excited (i.e., with high energy and very far from the ground state), as the problem size increases.

In the next section, we follow the *iterated reverse annealing*²² approach, which was studied numerically in a closed-system setting, and propose an iterative strategy for the DWave system to solve bigger problems. The goal is to converge to a low-energy state that can be used as the initial state for single-iteration RV to reach the global minimum with an effective pause T_p .

Solving prime factorization with iterated reverse annealing (IRV)

In general, we assume that starting reverse annealing from a state that is close to the ground state could be beneficial in finding the solution. We remark, however, that we have no prior knowledge of the solution. To cope with this missing information, we assumed that a low-energy state may be closer to the ground state and our proposal is built on top of this assumption.

The IRV strategy starts by running a standard forward annealing process, with thermal relaxation disabled. The obtained lowest-energy state is selected as the starting point for the subsequent iterations of the algorithm. At each iteration of the IRV, we execute a batch of RV processes, with several pause lengths T_p and pausing points S_p taken into consideration, until we obtain a lower-energy space. The *lower-energy space* refers to the set of lower-energy states retrieved in one iteration whose energy is *below* the starting point. Once that space has been retrieved, we check if there is a ground state in that space: when

Size	Input N	S_p	$\min(P_F)$	$\#(P_F = 0)$	Size	Input N	S_p	$\min(P_F)$	$\#(P_F = 0)$	Size	Input N	S_p	$\min(P_F)$	$\#(P_F = 0)$
8×8	49,447 (251×197)	0.38	0.000	1	9×8	100,273 (509×197)	—	4.083	0	10×8	201,137 (1021×197)	—	6.167	0
	49,949 (251×199)	—	4.083	0		101,291 (509×199)	—	8.083	0		203,179 (1021×199)	—	8.000	0
	52,961 (251×211)	—	6.000	0		107,399 (509×211)	—	4.000	0		215,431 (1021×211)	—	6.083	0
	55,973 (251×223)	0.33	0.000	6		113,507 (509×223)	—	8.083	0		227,683 (1021×223)	0.34	0.000	1
	56,977 (251×227)	0.33	0.000	1		115,543 (509×227)	0.33	0.000	1		231,767 (1021×227)	—	8.083	0
	57,479 (251×229)	0.33	0.000	3		116,561 (509×229)	—	6.000	0		233,809 (1021×229)	—	8.000	0
	58,483 (251×233)	—	6.083	0		118,597 (509×233)	—	4.000	0		237,893 (1021×233)	—	6.000	0
	59,989 (251×239)	0.33	0.000	43		121,651 (509×239)	0.33	0.000	1		244,019 (1021×239)	—	6.250	0
9×8	60,491 (251×241)	0.38	0.000	1	10×8	122,669 (509×241)	—	8.167	0	10×8	246,061 (1021×241)	—	6.167	0
	63,001 (251×251)	—	2.000	0		127,759 (509×251)	0.36	0.000	1		256,271 (1021×251)	0.35	0.000	2

(a) Prime factorization of 8×8 , 9×8 and 10×8 -bit numbers, with $T_a = 10\mu s$ and pause $T_p = 100\mu s$.

Size	Input N	Forward annealing		Reverse annealing		
		S_p	$\min(P_F)$	S'_p	P_F	$\#(P_F = 0)$
8×8	49,949 (251×199)	0.50	2.000	0.33	0.000	233
	52,961 (251×211)	0.35	2.000	0.41	0.000	177
	58,483 (251×233)	0.33	2.083	—	4.000	144
	63,001 (251×251)	0.51	2.000	0.35	0.000	168
9×8	100,273 (509×197)	0.36	4.000	—	4.083	198
	101,291 (509×199)	0.44	4.000	—	4.000	2
	107,399 (509×211)	0.51	4.000	—	4.000	79
	113,507 (509×223)	0.38	2.000	—	2.000	71
	116,561 (509×229)	0.36	4.000	0.37	0.000	98
	118,597 (509×233)	0.33	2.000	—	4.000	201
	122,669 (509×241)	0.48	4.083	0.36	0.000	129
10×8	201,137 (1021×197)	0.38	2.000	—	2.000	6
	203,179 (1021×199)	0.34	4.000	—	4.083	218
	215,431 (1021×211)	0.4	4.000	—	4.000	228
	231,767 (1021×227)	0.33	2.083	—	4.083	201
	233,809 (1021×229)	0.39	4.083	—	6.000	112
	237,893 (1021×233)	0.46	2.083	—	2.083	2
	244,019 (1021×239)	0.48	2.000	—	4.000	137
	246,061 (1021×241)	0.34	4.000	—	2.083	142

(b) Results of performing reverse annealing on the problem instances not solved in Table 3a, with $T_a = 10\mu s$ and $T_p = 10\mu s$. The label ΔHAM reports the Hamming distance between the forward annealing lowest energy sample and the reverse annealing lowest energy sample.

Table 3. Results about prime factorization solved through QA, exploiting thermal relaxation.

this happens, we have the solution for the problem and we stop the entire procedure; otherwise, this procedure is iterated until the system finds the ground state or hits a certain number of iterations.

It is not trivial to determine how long a pause should be and when to trigger it for the intermediate iterations to gradually approach the ground state. Based on the previous observations, we chose a set of pause lengths e.g., $\{1, 10, 30, 50, 100\}\mu s$ and a set of pause point, e.g., $\{0.46, \dots, 0.33\}$, adapting those parameters to the initial states of this iteration. We tested IRV on the DWave Advantage System 4.1 by trying to factorize the numbers 1,027,343, 4,111,631, and 16,445,771 using respectively a 12×8 , 14×8 , and 16×8 -bit multiplier. The experiments consider the assumptions discussed in the previous paragraphs, a further analysis of these conditions is left as future work. Table 4a reports the successful search paths of IRV in finding the ground state, demonstrating that IRV is effective in reaching a solution even from an excited state very far away from the minimum, by approaching it gradually. We highlight that from our experiments it was impossible for standard reverse annealing to factor 4,111,631 even with a $600\mu s$ pause.

We also propose a variant of the IRV strategy discussed above. From the failed factorization of 16,445,771, we noticed that the last iteration got stuck in the local minimum even with a pause of $100\mu s$. To cope with this issue, we opted to focus on triggering long distances. This is done by increasing the pause length at each iteration, i.e., $T_p \in \{100, 200\}\mu s$. Correspondingly, we simplify the choice of the starting state for an iteration, choosing the lowest-energy state as the initial state of each iteration. The experimental results shown in Table 4b demonstrate the improvement of this variant of IRV, in terms of fewer iterations required to reach the solution, at the cost of more QPU time. Notice that in the case of the 23-bit number, 8,219,999, we use a pause of $1\mu s$. This is due to the fact the initial state is highly excited and a $1\mu s$ pause can still trigger a relatively long distance, saving QPU time. According to the results in Table 4a, we highlight how the fourth iteration highly benefits from the long pause. Despite starting from a local minimum that is very far away from the solution, the long pause enables RV to travel long Hamming distances and reach a local minimum closer to our solution. This closer state provides a good initial state for the last-iteration RV to find the solution successfully.

Size	Input N	#	T_p	S_p	$\min(P_F)$	$\min(P_F)_{new}$	$(HAM, \Delta HAM, HAM_{new})$
12 × 8	1,027,343 (4093 × 251)	1	1	0.31	10.167	4.000	(263, 142, 151)
		2	1	0.38	10.167	4.083	(128, 122, 58)
		3	100	0.38	4.083	0[2]	(58, 58, 0)
14 × 8	4,111,631 (16381 × 251)	1	1	0.35	18.167	8.083	(290, 353, 249)
		2	1	0.35	16.000	6.000	(273, 219, 240)
		3	50	0.37	10.000	2.083	(277, 280, 85)
		4	10	0.38	2.083	0[67]	(85, 85, 0)
16 × 8	16,445,771 (251 × 65521)	1	1	0.34	18.333	6.083	(, 294,)
		2	10	0.35	10.000	4.000	(, 374,)
		3	50	0.36	6.083	4.167	(, 292,)
		4	100	0.39	4.167	4.000	(, 8,)

(a) Results of the original IRV algorithm. For the 16×8 problem, since no ground state has been retrieved, no comparison of Hamming distances with the ground state are provided (thus HAM and HAM_{new} are left empty).

Size	Input N	#	T_p	S_p	$\min(P_F)$	$\min(P_F)_{new}$	$(HAM, \Delta HAM, HAM_{new})$
13 × 8	2,055,941 (8191 × 251)	1	100	0.38	14.083	6.083	(204, 185, 55)
		2	100	0.42	6.083	0[216]	(55, 55, 0)
14 × 8	4,111,631 (16381 × 251)	1	200	0.39	16.167	6.083	(164, 178, 136)
		2	200	0.44	6.083	0[467]	(136, 136, 0)
15 × 8	8,219,999 (32749 × 251)	1	1	0.4	20.333	12.167	(279, 126, 217)
		2	100	0.43	12.167	8.000	(217, 180, 277)
		3	200	0.43	8.000	6.000	(277, 65, 282)
		4	200	0.44	6.000	4.083	(282, 247, 71)
		5	200	0.44	4.083	0[329]	(71, 71, 0)

(b) Results of the IRV variant that focuses on longer pauses.

Table 4. Result about IRV. The label ΔHAM reports the Hamming distance between the forward annealing lowest energy sample and the reverse annealing lowest energy sample. The labels HAM and HAM_{new} reports the Hamming distance of respectively the starting point and the lowest energy sample of that iteration with respect to the ground state. The bold number near 0 reports how many samples reached 0 energy for that iteration, out of 1000.

Overall, exploiting all the encoding and solving techniques described in this paper, $8,219,999 = 32,749 \times 251$ was the highest prime product we were able to factorize. To the best of our knowledge, this is the largest number that was ever factorized by means of quantum annealing.

Conclusions and Future Work

In this paper we have proposed a novel approach to prime factorization by quantum annealing. Our contribution is twofold.

First, we have presented a novel modular *encoding* of a binary multiplier circuit into the Pegasus architecture of the most recent D-Wave QA devices. The key to success was a compact encoding of a controlled full-adder sub-circuit into an 8-qubit module in the Pegasus topology, which we synthesized offline by means of Optimization Modulo Theories. This allows us to encode up to a 21×12 -bit multiplier (resp. a 22×8 -bit one) into a 5760-qubit Advantage 4.1 annealer. To the best of our knowledge, these are the largest factorization problems ever encoded into a quantum annealer. Also, due to the modularity of the encoding, this number will scale up automatically with the growth of the qubit number in future chips. Thus, we believe that this encoding can be used as a baseline for many future research for prime factorization via QA.

Second, we have investigated the problem of actually *solving* encoded PF problems by running an extensive experimental evaluation on a D-Wave Advantage 4.1 quantum annealer. Despite the presence of faulty qubits and couplings and within the limited amount of QPU time we had access to, by exploiting all the encoding and solving techniques we introduced and described in this paper, $8,219,999 = 32,749 \times 251$ was the highest prime product we were able to factorize. To the best of our knowledge, this is the largest number which was ever factorized by means of a quantum annealer, and more generally by a quantum device, without adopting hybrid quantum-classical techniques. We are confident that even better results can be obtained with a less-faulty annealer and a larger availability of QPU time.

There is still much room for further developments. First, efficient encodings for alternative multiplier schemata could be developed.¹³ Second, other solving strategies within the annealing process could be conceived and empirically investigated. Moreover, D-Wave recently announced the upcoming generation of quantum processors built on top of a new topology, Zephyr, that provides more connections and cliques among different sets of qubits. Once we have access to a large-enough Zephyr processor, we plan to test out encoding algorithms to get better penalty functions for the CFAs and reach global minima more easily during the solving phase.

Data availability

Data about the experimental section, and in particular the code to replicate the solving experiments is publicly accessible here: <https://gitlab.com/jingwen.ding/multiplier-encoder/>.

References

1. Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
2. Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134, DOI: [10.1109/SFCS.1994.365700](https://doi.org/10.1109/SFCS.1994.365700) (1994).
3. Vandersypen, L. M. K. *et al.* Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883–887, DOI: [10.1038/414883a](https://doi.org/10.1038/414883a) (2001).
4. Lucero, E. *et al.* Computing prime factors with a josephson phase qubit quantum processor. *Nat. Phys.* **8**, 719–723, DOI: [10.1038/nphys2385](https://doi.org/10.1038/nphys2385) (2012).
5. Martín-López, E. *et al.* Experimental realization of Shor’s quantum factoring algorithm using qubit recycling. *Nat. Photonics* **6**, 773–776, DOI: [10.1038/nphoton.2012.259](https://doi.org/10.1038/nphoton.2012.259) (2012).
6. Monz, T. *et al.* Realization of a scalable Shor algorithm. *Science* **351**, 1068–1070, DOI: [10.1126/science.aad9480](https://doi.org/10.1126/science.aad9480) (2016). <https://www.science.org/doi/pdf/10.1126/science.aad9480>.
7. Amico, M., Saleem, Z. H. & Kumph, M. Experimental study of Shor’s factoring algorithm using the ibm q experience. *Phys. Rev. A* **100**, 012305, DOI: [10.1103/PhysRevA.100.012305](https://doi.org/10.1103/PhysRevA.100.012305) (2019).
8. Selvarajan, R., Dixit, V. & Cui, X. e. a. Prime factorization using quantum variational imaginary time evolution. *Sci Rep* **11**, DOI: <https://doi.org/10.1038/s41598-021-00339-x> (2021).
9. Willsch, D., Willsch, M., Jin, F., De Raedt, H. & Michielsen, K. Large-scale simulation of Shor’s quantum factoring algorithm. *Mathematics* **11**, DOI: [10.3390/math11194222](https://doi.org/10.3390/math11194222) (2023).
10. Karamlou, A., Simon, W. & Katabarwa, A. e. a. Analyzing the performance of variational quantum factoring on a superconducting quantum processor. *Quantum Inf* **7**, DOI: <https://doi.org/10.1038/s41534-021-00478-z> (2021).
11. Dridi, R. & Alghassi, H. Prime factorization using quantum annealing and computational algebraic geometry. *Sci. Reports* **7**, 43048, DOI: [10.1038/srep43048](https://doi.org/10.1038/srep43048) (2017).
12. Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S. & Kais, S. Quantum annealing for prime factorization. *Sci. Reports* **8**, 17667, DOI: [10.1038/s41598-018-36058-z](https://doi.org/10.1038/s41598-018-36058-z) (2018).
13. Mengoni, R., Ottaviani, D. & Iorio, P. Breaking RSA security with a low noise D-Wave 2000Q quantum annealer: Computational times, limitations and prospects, DOI: <https://doi.org/10.48550/arXiv.2005.02268> (2020).
14. Wang, B., Hu, F. & Yao, H. e. a. Prime factorization algorithm based on parameter optimization of ising model. *Sci. Reports* **10** (2020).
15. Bian, Z. *et al.* Mapping constrained optimization problems to quantum annealing with application to fault diagnosis. *Front. ICT* **3**, DOI: [10.3389/fict.2016.00014](https://doi.org/10.3389/fict.2016.00014) (2016).
16. Bian, Z. *et al.* Solving SAT (and MaxSAT) with a quantum annealer: Foundations, encodings, and preliminary results. *Inf. Comput.* **275**, 104609, DOI: <https://doi.org/10.1016/j.ic.2020.104609> (2020).
17. Boothby, K., Bunyk, P., Raymond, J. & Roy, A. Next-generation topology of d-wave quantum processors. *D-Wave Tech. Rep. Ser.* **14-1026A-C** (2019-02-25).
18. Sebastiani, R. & Trentin, P. OptiMathSAT: A tool for optimization modulo theories. *J. Autom. Reason.* **64**, 423–460, DOI: [10.1007/s10817-018-09508-6](https://doi.org/10.1007/s10817-018-09508-6) (2020).
19. D-Wave Systems Inc. Flux-bias offsets. https://docs.dwavesys.com/docs/latest/c_qpu_error_correction.html#flux-bias-offsets.
20. Marshall, J., Venturelli, D., Hen, I. & Rieffel, E. G. Power of pausing: Advancing understanding of thermalization in experimental quantum annealers. *Phys. Rev. Appl.* **11**, 044083, DOI: [10.1103/PhysRevApplied.11.044083](https://doi.org/10.1103/PhysRevApplied.11.044083) (2019).
21. WHITEPAPER. Reverse quantum annealing for local refinement of solutions. *D-Wave Whitepaper Ser.* **14-1018A-A** (2017-11-09).
22. Yamashiro, Y., Ohkuwa, M., Nishimori, H. & Lidar, D. A. Dynamics of reverse annealing for the fully connected p -spin model. *Phys. Rev. A* **100**, 052321, DOI: [10.1103/PhysRevA.100.052321](https://doi.org/10.1103/PhysRevA.100.052321) (2019).