Resolution and Expressiveness of Subclasses of Quantified Boolean Formulas and Circuits

Hans Kleine Büning[1], Xishun Zhao[2], and Uwe Bubeck[1]

[1] Universität Paderborn, Germany. kbcsl@upb.de, bubeck@upb.de
[2] Sun Yat-sen University Guangzhou, PR China. hsszxs@mail.sysu.edu.cn

Abstract. We present an extension of Q-Unit resolution for formulas that are not completely in clausal form. This *b-unit resolution* is applied to different classes of quantified Boolean formulas in which the existential and universal variables satisfy the Horn property. These formulas are transformed into propositional equivalents consisting of only polynomially many subformulas. We obtain compact encodings as Boolean circuits and show that both representations have the same expressive power.

1 Introduction

Recently, there has been growing interest [7, 8] in non-clausal or structural quantified Boolean formulas (QBF or QBF* if free variables are allowed). Accordingly, we present an extension of Q-Unit resolution, denoted *b-unit resolution*, for formulas that are not completely in clausal form. We relate the idea to Boolean circuits which have the ability to use intermediate results in multiple places by fan-out, so that we avoid copying of resolvents in our b-unit resolution.

We begin with some definitions. A QBF* formula Φ is *satisfiable* if there is a truth assignment v to the free variables $\mathbf{z}$ such that Φ is true after substituting the truth values v for the free variables. For $\Phi \in$QCNF*, we write $\Phi = Q \bigwedge_i (\phi_i^b \vee \phi_i^f)$, where the *b-part* ϕ_i^b is a clause over bound variables and the *f-part* ϕ_i^f is a clause over free variables. QHORN* is the set of quantified Horn formulas with free variables, i.e. formulas $Q\phi$ where ϕ is a Horn formula. QHORN^b is the set of formulas where each b-part ϕ_i^b is a Horn clause and ϕ_i^f an arbitrary clause over free variables. QHORN$^+$ (QHORN$^-$) is the subset of QHORN^b for which the f-part of each clause is a disjunction of positive (negated) variables.

A circuit is a DAG with one outgoing edge and multiple input nodes labeled with Boolean variables. The other nodes are AND-, OR-, and NOT-gates that each have two (AND and OR) or one (NOT) incoming edges. The *fan-out* of a circuit is the maximum number of outgoing edges of the AND- and OR-gates. We can transform in linear time any circuit into *standard form*, where the inner nodes are only AND- and OR-gates and the inputs are variables x and/or negated variables $\neg x$. Subsequently, we focus on the class C of circuits in standard form.

A *monotone* propositional formula contains no negations. *Anti-monotone* formulas are negated monotone formulas. Analogously, *monotone* circuits $\mathcal{C}_{mon}$ have only non-negated variables as inputs. *Anti-monotone* circuits $\mathcal{C}_{anti-mon}$

have only negated inputs $\neg x$. Suppose we have Horn clauses $(\alpha_1 \to x)$, ..., $(\alpha_n \to x)$. We can combine these into $((\alpha_1 \vee \ldots \vee \alpha_n) \to x)$, which is not a Horn clause, but $(\alpha_1 \vee \ldots \vee \alpha_n)$ is monotone and thus equivalent to a monotone circuit. More generally, we introduce *$\mathcal{C}$-Horn clauses* $(c \to z)$, where c is a monotone propositional formula and z a variable. $(c \to z)$ can be represented as a circuit $(z \vee \neg c)$ with monotone c. This non-standard circuit can be transformed into $(z \vee c')$ in standard form, where $c' \approx \neg c$ and c' is anti-monotone. A conjunction $\bigwedge_i (c_i \to z_i)$ of circuits that represent $\mathcal{C}$-Horn clauses is called a $\mathcal{C}_{Horn}$ circuit.

For $i = 1, 2$, let $\Phi_i(\mathbf{z})$ be a propositional formula over variables $\mathbf{z}$, a QBF* formula with free variables $\mathbf{z}$, or a circuit with input variables $\mathbf{z}$. Then Φ_1 and Φ_2 are *equivalent* ($\Phi_1 \approx \Phi_2$) if and only if for every truth assignment v over $\mathbf{z}$ we have $v(\Phi_1) = v(\Phi_2)$. The *size* $|c|$ of a circuit c is the number of gates. For a formula Φ, $|\Phi|$ is its *length.* The usual definition is to count the number of occurrences of variables, including the prefix. Without multiple negations $(\neg\neg x)$, this differs only by a constant factor from the number of operators.

Definition 1. *For classes A, B of propositional or QBF* formulas or circuits, we let $A \leq_p^r B$ if and only if there is a polynomial q such that for any $\alpha \in A$ there is $\beta \in B$ with $\alpha \approx \beta$ and $|\beta| \leq q(|\alpha|)$. $A =_p^r B$ if $A \leq_p^r B$ and $B \leq_p^r A$.*

2 Extensions of Unit Resolution

It is well known that unit resolution is complete for Horn formulas. *Q-Unit resolution* [5] extends the idea to QCNF* by resolving on free and existential literals where one of the parent clauses has exactly one such literal. This is correct and refutation-complete [5] for formulas $\Phi = Q(\alpha_1 \wedge \ldots \wedge \alpha_m)$ with free variables $\mathbf{z}$ in which for every clause α_i the existential and free literals form a Horn clause, i.e. after eliminating all universals the clause is in HORN. Such formulas are called *quantified extended Horn* (QEHORN*). The satisfiability problem for this class has been shown to be PSPACE-complete in general and coNP-complete for a fixed number of prefix alternations $(\forall\exists)^k$, $k \geq 1$ [4]. There exist QEHORN formulas for which every resolution refutation requires exponentially many steps [5].

We now present an extension of Q-Unit resolution for formulas that are not completely in clausal form. Let $\Phi = Qv_1 \ldots Qv_n \bigwedge_i (\phi_i^b \vee \alpha_i)$ be in QBF*, where ϕ_i^b is a Horn clause over bound variables and α_i an arbitrary propositional formula over free variables. Then Φ is not in QHORN^b if α_i is not a disjunction of literals. But ϕ_i^b is a Horn formula on which we can apply unit resolution.

Definition 2. *We say that $(L \vee \alpha)$ is a* b-unit clause *if L is a literal over an existentially quantified variable and α is a formula over free variables.*

Let $(L \vee \alpha_1)$ be a b-unit clause, $(\neg L \vee \beta)$ a Horn clause over bound variables, and α_2 a formula over free variables. Then we define b-unit resolution *as*

$$(L \vee \alpha_1), (\neg L \vee \beta \vee \alpha_2) \;\vdash^{1}_{\textit{b-Unit-Res}}\; (\beta \vee \alpha_1 \vee \alpha_2) \ .$$

Q-Unit resolution is only refutation complete in combination with universal reduction, that is, the removal of universals that do not dominate any existential in the same clause. We also have to be careful not to resolve clauses with tautological universals. Such blockings usually require detours in resolution derivations, making them longer. While $\exists$-unit clauses in Q-Unit resolution may have an arbitrary number of universals, our definition of b-unit resolution avoids these difficulties by requiring that b-unit clauses have exactly one bounded literal which is existential. This is justified by the following result on QHORN^b formulas.

It has been shown in [3] that any QHORN* formula Φ can be transformed into an equivalent $\Phi' \in \exists$HORN*, such that the length of Φ' and the time for executing the transformation are less than quadratic in $|\Phi|$. That proves QHORN$^* =_p^r \exists$HORN*. A careful analysis of the transformation shows that the free parts of the clauses remain unchanged. Thus, $\exists$HORN$^- =_p^r$ QHORN$^-$. For $\Phi \in$ QHORN$^+$, we substitute the positive occurrences of free variables by their complements. Then the formula is in QHORN$^-$ and has an equivalent formula in $\exists$HORN$^-$ of at most quadratic length. We reverse the substitution and obtain a formula in $\exists$HORN$^+$ equivalent to Φ and with length at most quadratic in $|\Phi|$.

For QHORN$^b \leq_p^r \exists$HORN^b, let $\Phi(\mathbf{z}) = Q\ (\bigwedge_{1\leq i\leq m}(\phi_i^b \vee \phi_i^f))$ be a QHORN^b formula. We introduce for each clause a new variable w_i and replace ϕ_i^f with $\neg w_i$. We get the QHORN$^-$ formula $\Phi(\mathbf{w}) = Q \bigwedge_{1\leq i\leq m}(\phi_i^b \vee \neg w_i)$. Because of $\exists$HORN$^- =_p^r$ QHORN$^-$, there is an $\exists$HORN$^-$ formula $\Phi'(\mathbf{w}) = \exists \mathbf{y} \bigwedge_j (\varphi_j^b \vee \varphi_j^f)$ of quadratic length with $\Phi(\mathbf{w}) \approx \Phi'(\mathbf{w})$. For $1 \leq i \leq m$, we now replace $\neg w_i$ with ϕ_i^f and obtain for $(\varphi_j^b \vee \neg w_{i_1} \vee \cdots \vee \neg w_{i_r})$ the clause $(\varphi_j^b \vee \phi_{i_1}^f \vee \cdots \vee \phi_{i_r}^f)$. The result is equivalent to Φ and is in $\exists$HORN^b with length polynomial in $|\Phi|$.

Lemma 1. $\exists$HORN$^\circ =_p^r$ QHORN$^\circ$ *for* $\circ \in \{*, b, +, -\}$ *by polynomial-time transformations.*

Each step of b-unit resolution can be simulated by a series of regular Q-Unit resolution steps. Let $Q\phi = Q(\phi' \wedge (L \vee \alpha_1) \wedge (\neg L \vee \beta \vee \alpha_2))$ be the formula which contains the two extended clauses to be resolved. Then we transform $(L \vee \alpha_1)$ into an equivalent conjunction of clauses $(L \vee \alpha_{1,1}) \wedge ... \wedge (L \vee \alpha_{1,r})$, and similarly $(\neg L \vee \beta \vee \alpha_2)$ into $(\neg L \vee \beta \vee \alpha_{2,1}) \wedge ... \wedge (\neg L \vee \beta \vee \alpha_{2,s})$. Now we perform all possible Q-Unit resolutions over L. The definition of Q-Unit resolution implies $Q\psi \approx Q(\psi \wedge \sigma)$ for every resolvent σ [6]. In our case, it follows that $Q\phi \approx Q(\phi \bigwedge_{i,j}(\beta \vee \alpha_{1,i} \vee \alpha_{2,j}))$. Since all resolvents contain β, we pull it out $\bigwedge_{i,j}(\beta \vee \alpha_{1,i} \vee \alpha_{2,j}) \approx \beta \vee \bigwedge_{i,j}(\alpha_{1,i} \vee \alpha_{2,j})$. Now we can reverse the CNF transformation of α_1 and α_2: $\beta \vee \bigwedge_{i,j}(\alpha_{1,i} \vee \alpha_{2,j}) \approx \beta \vee \bigwedge_i(\alpha_{1,i} \vee \bigwedge_j \alpha_{2,j}) \approx \beta \vee \bigwedge_i(\alpha_{1,i} \vee \alpha_2) \approx \beta \vee \alpha_1 \vee \alpha_2$, which is the b-unit resolvent as defined above.

Proposition 1. *Let* $\Phi = Q\phi$ *be a QBF* formula, and let* σ *be a b-unit resolvent* $\Phi \mid\frac{1}{\textit{b-Unit-Res}}\ \sigma$. *Then we have* $Q\phi \approx Q(\phi \wedge \sigma)$.

So, b-unit resolution is a way to perform multiple unit resolution steps at once. We attempt to make even more use of this capability by actively combining multiple b-unit clauses with the same bound variable into a larger b-unit clause.

Definition 3. *Let* $\varphi = \{F_{1,1} \to x_1 ... F_{r_1,1} \to x_1, ..., F_{1,m} \to x_m ... F_{r_m,m} \to x_m\}$ *be a set of b-unit clauses.* $F_{i,j}$ *contains only free variables, and* x_j *is bound.*
We define $cmb(\varphi) := \{(F_{1,1} \vee \ldots \vee F_{r_1,1}) \to x_1, \ldots, (F_{1,m} \vee \ldots \vee F_{r_m,m}) \to x_m\}$.

3 Structure of Resolvents and Circuits

We now want to derive by b-unit resolution from a given $\exists$HORN* formula a quantifier-free formula $(F \to z)$ where F is a monotone propositional formula. While F may have exponential size, we show that it essentially consists of only at most quadratically many different subformulas, because it can be derived by a quadratic number of b-unit resolution steps, where each resolvent can be represented by a linear-size circuit. By fan-out greater than 1, the substitution of one resolvent into another one can be performed without copying. The ability of b-unit resolution to work on non-CNF avoids subformulas being torn apart by repeated CNF transformation. The following example illustrates the idea:
Let $\Phi = \exists x_1 \exists x_2 \exists x_3 \exists y\ (\neg y \vee z) \wedge (a \to x_1) \wedge (b \to x_1) \wedge (c \wedge x_1 \to y) \wedge (d \wedge x_1 \to x_3)$. Φ contains the b-units $T(0) := \{(a \to x_1), (b \to x_1)\}$. We combine these into $G(0) := \{(a \vee b) \to x_1\}$. Then we resolve the units in $G(0)$ with the clauses in Φ by b-unit resolution and get $T(1) := \{(c \wedge (a \vee b) \to y), (d \wedge (a \vee b) \to x_3)\} \cup T(0)$. The combined b-units are $G(1) := \{((a \vee b) \to x_1), (c \wedge (a \vee b) \to y), (d \wedge (a \vee b) \to x_3)\}$. Further propagation does not lead to new combined b-units. Finally, we resolve on the clause $(\neg y \vee z)$ with negative b-part and get $T^f = ((c \wedge (a \vee b)) \to z) \approx \Phi$. This leads to the algorithm in Listing 1.

Listing 1: $\exists$HORN* to C_{Horn} Transformation

Input $\Phi(\mathbf{z}) = \exists \mathbf{x} \phi \in \exists$HORN* with free variables $\mathbf{z} = z_0, \ldots, z_m$
and n clauses, each containing a bound variable.
$\Phi^b = \exists \mathbf{x} \phi^b$ is unsatisfiable, ϕ contains exactly one clause
$\phi_1 = (B_1 \to z_0)$ whose bound part is a negative clause;

$T(0)$:= $\{(F \to x) \in \phi \mid x$ bound, F has only (positive) free vars$\}$;
$G(0)$:= $cmb(T(0))$;
for each $(F \to x) \in G(0)$
  build a monotone circuit $c_x(0) \approx F$ with output labeled x;
for (k = 0 to n) {
  $T(k+1)$:= $\{\psi[x_1/F_1, \ldots, x_r/F_r] \to x \mid (\psi \to x) \in \phi,\ (F_i \to x_i) \in G(k),$
      $x_1, \ldots, x_r$ are the bound variables in ψ, x is bound$\}$
  for each $(\psi' \to x) \in T(k+1)$
    build a monotone circuit $c_{\psi'}(k+1) \approx \psi' = \psi[x_1/F_1, \ldots, x_r/F_r]$
    with output labeled ψ' by reusing the circuits $c_{x_i}(k)$;
  $G(k+1)$:= $cmb(G(k) \cup T(k+1))$;
  for each $(F \to x) \in G(k+1)$
    build a monotone circuit $c_x(k+1) \approx F$ with output labeled x
    by reusing the circuits $c_{x_i}(k)$ and $c_{\psi'_j}(k+1)$;
}
T^f := $(B_1[x_1/F_1, \ldots, x_r/F_r] \to z_0)$
  where $x_1, \ldots, x_r$ are the bound variables in the distinguished
  clause $(B_1 \to z_0)$ and $(F_i \to x_i) \in G(n+1)$;
combine circuits $c_{x_1}(n+1), \cdots, c_{x_r}(n+1)$ by AND–gates into a
monotone circuit $c_\Phi \approx B_1[x_1/F_1, \ldots, x_r/F_r]$;

Output C_{Horn} circuit $c \approx z_0 \vee \neg c_\Phi$. It follows that $c \approx \Phi(\mathbf{z})$.

The algorithm requires some initial transformations. Each $\Phi = Q \bigwedge_i (\phi_i^b \vee \phi_i^f)$ can be converted in polynomial time into an equivalent formula such that every f-part contains at most one literal. Let $\phi_i^f = (\alpha \vee \beta)$ and $\phi_i^b = (\varphi_1 \vee \varphi_2)$ where φ_1 and φ_2 contain the negative and the positive literals, respectively. Then we introduce a new bound variable y and replace ϕ_i with $(\varphi_2 \vee \neg y \vee \alpha)$ and $(\varphi_1 \vee y \vee \beta)$. The monotone or anti-monotone structure of the f-parts and the Horn structure of the b-parts is preserved. So we assume that the clauses in QHORN* (QHORN$^+$, QHORN$^-$, QHORN^b) formulas contain at most one free literal such that the complete clause is a Horn clause (the f-part is a positive literal, the f-part is a negative literal, the f-part is an arbitrary free literal). Clauses $\phi_j = \phi_j^f$ can be shifted before the prefix, such that $\Phi \approx \phi_j \wedge Q \bigwedge_{i \neq j} \phi_i$. We therefore focus on formulas in which every clause contains a bound variable. We also require that every bound variable has at least one positive and one negative occurrence.

We can decide in linear time whether the conjunction $\Phi^b := \bigwedge_i \phi_i^b$ of all b-parts is satisfiable, because Horn satisfiability is solvable in linear time. If Φ^b is indeed satisfiable, $\Phi(\mathbf{z})$ is true for any truth assignment to the free variables and can be replaced by $(z \vee \neg z)$. Hence, we assume that Φ^b is unsatisfiable. Since any minimal unsatisfiable Horn formula contains exactly one negative clause in addition to the mixed clauses, we divide the formula into multiple subformulas that each contain a single negative clause ϕ_i^b. Suppose Φ has the negative b-parts $\phi_1^b, \dots, \phi_r^b$. Let $\phi' := \phi - \{\phi_1, \dots, \phi_r\}$. Then $\exists \mathbf{x} \phi \approx \exists \mathbf{x}(\phi' \wedge \phi_1) \wedge \dots \wedge \exists \mathbf{x}(\phi' \wedge \phi_r)$.

The clauses ϕ_i have the form $\phi_i = (\neg x_{j_1} \vee \dots \vee \neg x_{j_s} \vee \neg z_{k_1} \vee \dots \vee \neg z_{k_t} \vee z_0)$ for free variables $z_{k_1}, \dots, z_{k_t}, z_0$. W.l.o.g., we assume $\phi_i = (\neg x_{j_1} \vee \dots \vee \neg x_{j_s} \vee z_0)$ without negative free variables. If that were not the case for some ϕ_i, we could split it into $(\neg x_{j_1} \vee \dots \vee \neg x_{j_s} \vee \neg z_{k_1} \vee \dots \vee \neg z_{k_t} \vee \tilde{x})$ and $(\neg \tilde{x} \vee z_0)$ by introducing a new bound variable $\tilde{x}$. Now the only clause with negative b-part is $(\neg \tilde{x} \vee z_0)$.

From Listing 1, it is clear that the size of the circuit $c_\Phi \to z_0$ is polynomial in $|\phi|$, because the number of b-units in $T(i)$ and $G(i)$, $0 \leq i \leq n+1$, is each bounded by the number of clauses in Φ, and each circuit that represents one of these b-units has linear size due to the reusing of existing circuits. The equivalence of Φ and T^f follows in the direction from left to right immediately from Proposition 1. In the other direction, it is possible to show that for truth assignments V with $V \models T^f$, V implies enough left hand sides of b-unit clauses $(F_i \to x_i) \in G(n+1)$ such that ϕ is satisfied by V and $x_i = 1$ for these x_i.

Theorem 1. *Let $\Phi = \exists \mathbf{x} \phi$ be the input to the transformation in Listing 1. In polynomial time, the algorithm computes T^f with $T^f \approx \exists \mathbf{x} \phi$. T^f can be represented by a C_{Horn} circuit of polynomial size, and thus, $\exists$HORN* $\leq_p^r \mathcal{C}_{Horn}$.*

Any $\Phi \in \exists$HORN$^-$ is in $\exists$HORN* without positive free literals. Then the algorithm produces a disjunction of anti-monotone circuits $c_1, \dots, c_r$. The disjunction of anti-monotone circuits is again anti-monotone, so $\exists$HORN$^-$ $\leq_p^r \mathcal{C}_{anti-mon}$.
For $\Phi \in \exists$HORN$^+$, we replace the free literals with their complements and obtain a formula in $\exists$HORN$^-$ and then an equivalent anti-monotone circuit. We reverse the substitution and obtain a monotone circuit. Then $\exists$HORN$^+$ $\leq_p^r \mathcal{C}_{mon}$.
For $\Phi \in \exists$HORN^b, the f-parts ϕ_i^f are arbitrary clauses over free variables. For

each ϕ_i, we choose a new variable w_i that replaces ϕ_i^f. The result is in $\exists$HORN$^+$, and there is an equivalent monotone circuit c. For each ϕ_i^f, we build an equivalent circuit c_i with output y_i and connect it to the input w_i of c. The new circuit is equivalent to Φ, and its size is polynomial in $|\Phi|$. Thus, $\exists\text{HORN}^b \leq_p^r \mathcal{C}$.

The well-known transformation of circuits to formulas [1, 2] produces $\exists$HORN^b formulas. A close look at these for monotone, anti-monotone and C_{Horn} circuits shows that the above polynomial-size relations also hold in the other direction.

Theorem 2. *(Quantified Horn Formulas and Circuits)*
By polynomial-time transformations, we have:

1. $\text{QHORN}^+ =_p^r \exists\text{HORN}^+ =_p^r \mathcal{C}_{mon}$
2. $\text{QHORN}^- =_p^r \exists\text{HORN}^- =_p^r \mathcal{C}_{anti-mon}$
3. $\text{QHORN}^* =_p^r \exists\text{HORN}^* =_p^r \mathcal{C}_{Horn}$
4. $\text{QHORN}^b =_p^r \exists\text{HORN}^b =_p^r \mathcal{C}$

The latter constitutes an alternative proof to an earlier result $\exists\text{HORN}^b =_p^r \mathcal{C}$ by Anderaa and Börger [1], which is based on the fact that Horn satisfiability is solvable by a polynomial-time deterministic Turing machine, which in turn can be encoded by a uniform family of polynomial-size circuits.

4 Conclusion

By developing b-unit resolution for formulas that are not completely in clausal form, we have shown that various classes of quantified Boolean formulas in which the bound variables satisfy the Horn property can be transformed into quantifier-free formulas consisting of only polynomially many subformulas. These have compact encodings as circuits, and vice versa, which shows that both representations have the same expressive power, even if universal quantifiers are allowed.

References

[1] S. Anderaa and E. Börger. *The Equivalence of Horn and Network Complexity for Boolean Functions.* Acta Informatica, 15:303–307, 1981.

[2] M. Bauer, D. Brand, M. Fischer, A. Meyer, and M. Paterson. *A Note on Disjunctive Form Tautologies.* SIGACT News, 5(2):17–20, 1973.

[3] U. Bubeck and H. Kleine Büning. *Models and Quantifier Elimination for Quantified Horn Formulas.* Discrete Applied Mathematics, 156(10):1606–1622, 2008.

[4] A. Flögel, M. Karpinski, and H. Kleine Büning. *Subclasses of Quantified Boolean Formulas.* Proc. CSL 1990, Springer LNCS 533, pp. 145–155, 1990.

[5] A. Flögel, M. Karpinski, and H. Kleine Büning. *Resolution for Quantified Boolean Formulas.* Information and Computation, 117(1):12–18, 1995.

[6] M. Karpinski, H. Kleine Büning, and P. Schmitt. *On the computational complexity of quantified Horn clauses.* Proc. CSL 1987, Springer LNCS 329, pp. 129–137, 1987.

[7] F. Lonsing and A. Biere. *Nenofex: Expanding NNF for QBF Solving.* Proc. SAT 2008, Springer LNCS 4996, pp. 196–210, 2008.

[8] A. Sabharwal, C. Ansotegui, C. Gomes, J. Hart, and B. Selman. *QBF Modeling: Exploiting Player Symmetry for Simplicity and Efficiency.* Proc. SAT 2006, Springer LNCS 4121, pp. 382–395, 2006.