# An Interactive Proof System for TQBF

This material was presented in class on April 5 and 7, 2016.

We wish to revise the interactive proof system for coSAT that was given in class on March 31, 2016, so that it works for TQBF. The existence of such a proof system implies that PSPACE is contained in IP.

We follow the argument on pages 161 and 162 of your textbook. That argument is clear until it gets to the last displayed formula on page 161. Because the displayed expression should be the fully arithmetized and linearized version of the TQBF instance $\psi$, it should be

$$\Pi_{X_1} L_1 \Sigma_{X_2} L_1 L_2 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_1, X_2, \ldots . X_n). \tag{1}$$

Here and throughout this lecture, the products and sums are computed over $X_i \in \{0,1\}$, where 0 and 1 are elements of the field $\mathbb{Z}_p$, and $p$ is a suitably large prime. (The size of $p$ will be addressed below.) Assume without loss of generality that $\phi$ is a 3CNF formula on $n$ boolean variables with $m$ clauses.

The proof system for TQBF needs $i+1$ *segments* of interaction, say $(i.1)$ through $(i.i+1)$, between Arthur and Merlin in order to handle $O_{X_i} L_1 L_2 \cdots L_i$, for $1 \le i \le n$, where $O = \Pi$ if $i$ is odd and $O = \Sigma$ is $i$ is even; each segment requires $O(1)$ rounds. (Think of a segment as a subprotocol.) So the entire protocol requires $O(n^2)$ rounds of interaction. The segment $(i.1)$ handles the operator $\Pi_{X_i}$, if $i$ is odd, and it handles the operator $\Sigma_{X_i}$, if $i$ is even. Subsequent segments $(i.2)$ through $(i.i+1)$ handle the operators $L_1$ through $L_i$.

Merlin's original claim is that the formula $\psi$ is true, which is equivalent to

$$\Pi_{X_1} L_1 \Sigma_{X_2} L_1 L_2 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_1, X_2, \ldots . X_n) \equiv C \bmod p, \tag{1.1}$$

where $C \neq 0$.

We now specify the first few segments of the proof system in detail:

Segment 1.1:

Note that Merlin's claim (congruence (1.1) above) is equivalent to the claim that $\Pi_{X_1}(h_1^1(X_1)) \equiv C \bmod p$, where $h_1^1$ is the linear, univariate polynomial in $X_1$ that results from evaluating all of the operators in congruence (1.1) except $\Pi_{X_1}$.

Arthur challenges Merlin to send him $h_1^1(X_1)$. Merlin sends him a linear, univariate polynomial $s_1^1(X_1)$. As in the sum-check protocol used in the proof system for coSAT, $s_1^1$ will be equal to $h_1^1$ if and only if Merlin is making a correct claim.

Arthur checks that $s_1^1(0) \cdot s_1^1(1) \equiv C \bmod p$; he rejects and halts the protocol if this check fails. Otherwise, he chooses $a_1^1$ uniformly at random from $\mathbb{Z}_p$ and sends it to Merlin.

Segment 1.2:

Merlin's claim is that

$$\Big[L_1 \Sigma_{X_2} L_1 L_2 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_2, \ldots . X_n)\Big](a_1^1) \equiv s_1^1(a_1^1) \bmod p. \tag{1.2}$$

This is equivalent to the claim that $\big[L_1(h_1^2)\big](a_1^1) \equiv s_1^1(a_1^1) \bmod p$, where $h_1^2(X_1)$ is the quadratic,[1] univariate polynomial in $X_1$ that results from evaluating all of the operators in congruence (1.2) except the leftmost $L_1$.

Arthur challenges Merlin to send him $h_1^2(X_1)$. Merlin sends him a quadratic, univariate polynomial $s_1^2(X_1)$. It will be equal to $h_1^2$ if and only if Merlin is making a correct claim.

Arthur checks that $(1-a_1^1)\cdot s_1^2(0)+a_1^1\cdot s_1^2(1) \equiv s_1^1(a_1^1)$ mod $p$; he rejects and halts the protocol if this check fails. Otherwise, he chooses $a_1^2$ uniformly at random from $\mathbb{Z}_p$ and sends it to Merlin.

Segment 2.1:
Merlin's claim is that

$$\Big[\Sigma_{X_2} L_1 L_2 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_1, X_2, \ldots . X_n)\Big](a_1^2) \equiv s_1^2(a_1^2) \bmod p. \qquad (2.1)$$

This is equivalent to the claim that $\Sigma_{X_2}(h_2^1(X_2)) \equiv s_1^2(a_1^2) \bmod p$, where $h_2^1$ is the linear, univariate polynomial in $X_2$ that results from evaluating all of the operators in congruence (2.1) except $\Sigma_2$.

Arthur challenges Merlin to send him $h_2^1$. Merlin sends him a linear, univariate polynomial $s_2^1$ in $X_2$. It will be equal to $h_2^1$ if and only if Merlin is making a correct claim.

Arthur checks that $s_2^1(0) + s_2^1(1) \equiv s_1^2(a_1^2)$ mod $p$; he rejects and halts the protocol if this check fails. Otherwise, he chooses $a_2^1$ uniformly at random from $\mathbb{Z}_p$ and sends it to Merlin.

Segment 2.2:
Merlin's claim is that

$$\Big[L_1 L_2 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_1, \ldots . X_n)\Big](a_1^2, a_2^1) \equiv s_2^1(a_2^1) \bmod p. \qquad (2.2)$$

This is equivalent to the claim that $\big[L_1(h_1^3)\big](a_1^2) \equiv s_2^1(a_2^1)$ mod $p$, where $h_1^3$ is the quadratic, univariate polynomial in $X_1$ that results from evaluating all of the operators in congruence (2.2) except the leftmost $L_1$.

Arthur challenges Merlin to send him $h_1^3$. Merlin sends him $s_1^3$. It will be equal to $h_1^3$ if and only if Merlin is making a correct claim.

Arthur checks that $(1-a_1^2)\cdot s_1^3(0)+a_1^2\cdot s_1^3(1) \equiv s_2^1(a_2^1)$ mod $p$; he rejects and halts the protocol if this check fails. Otherwise, he chooses $a_1^3$ uniformly at random from $\mathbb{Z}_p$ and sends it to Merlin.

Segment 2.3:
Merlin's claim is that

$$\Big[L_2 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_1, \ldots . X_n)\Big](a_1^3, a_2^1) \equiv s_2^2(a_1^3) \bmod p. \qquad (2.3)$$

This is equivalent to the claim that $\big[L_2(h_2^2)\big](a_2^1) \equiv s_2^2(a_1^3)$ mod $p$, where $h_2^2$ is the quadratic, univariate polynomial in $X_2$ that results from evaluating all of the operators in congruence (2.3) except the leftmost $L_2$.

[1] The question of why (and, in fact, whether) $h_1^2$ is quadratic is addressed below.

Arthur challenges Merlin to send him $h_2^2$. Merlin sends him $s_2^2$. It will be equal to $h_2^2$ if and only if Merlin is making a correct claim.
Arthur checks that $(1-a_2^1)\cdot s_2^2(0)+a_2^1\cdot s_2^2(1) \equiv s_2^2(a_1^3) \bmod p$; he rejects and halts the protocol if this check fails. Otherwise, he chooses $a_2^2$ uniformly at random from $\mathbb{Z}_p$ and sends it to Merlin.

Segment 3.1:
Merlin's claim is that

$$\Big[\Pi_{X_3} L_1 L_2 L_3 \cdots \Sigma_{X_n} L_1 L_2 \cdots L_n P_\phi(X_1 \ldots . X_n)\Big](a_1^3, a_2^2) \equiv s_2^3(a_2^2) \bmod p. \qquad (3.1)$$

. . . and so forth.

In general, we proceed in a similar fashion in segments $(i.1)$ through $(i.i+1)$. Segment $(i.1)$ handles operator $O_{X_i}$, where $O = \Pi$ if $i$ is odd and $O = \Sigma$ if $i$ is even. In segment $(i.1)$, Merlin is challenged to supply $h_i^1$, which is a univariate polynomial in $X_i$. If the $s_i^1$ that he supplies passes the required product or sum check, then Arthur chooses $a_i^1$ uniformly at random and sends it to Merlin. In segment $(i.j)$, for $2 \leq j \leq i+1$, Merlin is asked to supply $h_{j-1}^{i-j+3}$, which is a univariate polynomial in $X_{j-1}$. If the polynomial $s_{j-1}^{i-j+3}$ that he supplies passes the required linearity test, then Arthur chooses $a_{j-1}^{i-j+3}$ uniformly at random and sends it to Arthur. Note that segment $(i.1)$ is the first segment in which Merlin is asked to supply a polynomial in $X_i$ (specifically $h_i^1$) and that segment $(i.i+1)$ is the second time that Merlin is asked to supply a polynomial in $X_i$ (specifically, $h_i^2$, which is $h_{j-1}^{i-j+3}$, when $j$ is set to $i+1$). In general, the subscript $i$ on an $h$, $s$, or $a$ indicates the variable $X_i$, and the superscript $k$ indicates that this is the $k^{th}$ time that an $h$, $s$, or $a$ was chosen for the variable $X_i$. Whenever Merlin or Arthur has to plug in an $a_i^k$ for the variable $X_i$, he plugs in the most recently chosen one (*i.e.*, he plugs in $a_i^k$ for the highest value of $k$ that has been used thus far on this $i$).

Clearly, if Merlin is making a correct claim that the original TQBF instance $\psi$ is true, he can always convince Arthur to accept simply by answering all questions truthfully.

We now argue that, if Merlin's original claim is false, he can convince Arthur to accept only with exponentially small probability.

Note that we arithmetize $\phi$ using the arithmetization of Section 8.3.2. So each clause of $\phi$, which is a disjunction of three literals, is mapped to a factor of $P_\phi$ that is of degree at most three in each variable. The entire multivariate polynomial $P_\phi$ is the product of $m$ such factors and thus of degree at most $3m$ in each variable. It is not difficult to see that this implies that the univariate polynomial $h_i^j$ that is checked in each segment is also of degree at most $3m$.

If the proof system continues long enough, there will be few enough operators in the expression about which Merlin is making a claim to enable Arthur simply to check the correctness of the claim directly in polynomial time. Arthur will reject at this point if the claim that Merlin is making is false. Therefore, if Merlin starts with a false claim about $\psi$ and continues making false claims in every segment, Arthur will eventually reject. The only way that Merlin can get Arthur ultimately to accept is by switching at some point from making a false claim in one segment to making a true one in the next: If Merlin ever switches to a true claim, he can continue to do so until the end of the protocol.

How might Merlin get into a situation in which he can start making true claims? He must, when asked by Arthur to send a univariate polynomial $h_i^j$, send a polynomial $s_i^j \neq h_i^j$, because $s_i^j$ must pass a product, sum, or linearity test that $h_i^j$ would not pass. If $s_i^j$ agrees with $h_i^j$ on the next $a \in \mathbb{Z}_p$ chosen by Arthur, however, then Merlin is left with a true claim. Both $h_i^j$ and $s_i^j$ are univariate polynomials of degree at most $3m$; therefore, they can agree on at most $3m$ points. The value $a$ is chosen uniformly at random by Arthur from $\mathbb{Z}_p$, which is of size exponential in $m$ and $n$, *after* Merlin chooses $s_i^j$. Thus Merlin has an exponentially small chance of "lucking into" a correct claim in each segment. There are $O(n^2)$ segments, which implies that Merlin's total probability of getting Arthur to accept an incorrect claim that the original formula $\psi$ is true is exponentially small.

In the case of a segment $i.j$ in which the operator being handled is $L_{j-1}$, why might the polynomial $h_i^j$ be quadratic? Reading the sequence of operators in the congruence $(i.j)$ from right to left, consider what has happened as all operators except the leftmost $L_{j-1}$ have been evaluated. After the previous $L_{j-1}$ was evaluated (at which point the partial result was a multivariate polynomial that was linear in $X_{j-1}$), an arithmetic operator was applied. If that was a product operator, then it produced a multivariate polynomial that is quadratic in $X_{j-1}$. This degree doubling does not occur if the intervening arithmetic operator is a sum. However, it is more convenient to have a uniform specification for the protocol segments, and we can do so if we make the worst-case assumption that $h_i^j$ is quadratic. A linear polynomial is in fact just a quadratic polynomial with leading coefficient 0, and applying the linearization operator to a polynomial that is already linear just leaves it unchanged.

It remains to explain why it suffices to use a prime $p$ that is singly exponential in $n$ and $m$ (i.e., a $p$ that can be represented using a number of bits that is polynomial in $n$ and $m$). If we use the arithmetization from the interactive proof system for #SAT in Section 8.3.2 (not the arithmetization that we used in our interactive proof system for coSAT), then (1), evaluated over $\mathbb{Z}$, is equal to 0 if $\psi$ is false and 1 if $\psi$ is true. Therefore, wraparound is not an issue, and (1) has the correct value modulo $p$ for any $p$. Because the error probability is 0 in the case that Merlin is making a correct claim and $\frac{poly(n,m)}{p}$ in the case that Merlin is lying, we can use any $p$ that is singly exponential in $n$ and $m$.