Мы смотрим на доказательства корректности метода резолюций Res. Корректность любой системы доказательств можно записать в виде формулы (для фиксированных $r, n, m$), так называемой Reflection Principle:

$$SAT^n_r(x, z) \wedge REF^n_{r,m}(x, y),$$

где $r$ — количество клозов в формуле, $n$ — количество переменных в ней, $m$ — длина опровержения $y$ для $x$. $x$ здесь длины $r \times n \times 2$ кодирует саму формулу — $x_{i,v,b} = 1$ тогда и только тогда, когда переменная $v$ (если $b = 1$, то с отрицанием, иначе положительно) входит в $i$-й клоз формулы. $z$ кодирует выполняющий набор, но он не длины $n$, а длины $n + 2rn$ — там еще для каждого клоза хранится, какой литерал его выполняет. $SAT^n_r(x, z)$ просто проверяет, что $z$ правда кодирует выполняющий набор формулы, которую, в свою очередь, кодирует $x$.

$y$ же кодирует доказательство невыполнимости формулы в резолюциях — там так же кодируются клозы, плюс информация, из резолюции каких клозов очередной клоз был получен, и по какой переменной резолюция происходила. $REF^n_{r,m}(x, y)$ проверяет, что $y$ кодирует опровержение $x$ в Res. Получается, что если Res корректна, то Reflection Principle невыполнима — ведь если фиксировать формулу, то есть $x$, то нельзя одновременно выполнить и $SAT$, и $REF$, то есть подобрать и выполняющий набор $z$, и опровержение $y$.

Получается, чтобы доказать, что в Res нельзя опровергнуть выполнимые формулы, можно доказать невыполнимость Reflection Principle. Это и будет наш способ доказательство корректности. Вообще говоря, есть всякие теоремы о том, что из существования короткого опровержения Reflection Principle для системы доказательств A в системе доказательств B следуют всякие связи автоматизируемости этих систем, но это не то, о чем речь шла на семинаре.

Сначала мы доказали, что Reflection Principle для Res имеет короткое доказательство в Res[2]. Res[$k$] — это те же Res, только есть дополнительные переменные, которые соответствуют конъюнкциям не более, чем $k$ исходных литералов. Другими словами, в Res[$k$] можно клозы делать не просто дизъюнкцией литералов (то есть формулами в 1-CNF), а формулами в $k$-CNF. Правила там самые естественные — если мы вывели $l_i \vee C$ и $l_j \vee C$, то выводим $(l_i \wedge l_j) \vee C$, и наоборот, из последнего можно вывести $l_i \vee C$ и $l_j \vee C$. Все правила для Res сохраняются. Это и есть, на пальцах, определение Res[2]. Как проходило доказательство писать не буду, там просто много-много техники.

Потом мы доказали, что Reflection Principle для Res в Res коротко не опровергается. Для этого мы пользуемся тем, что графы, содержащие клики размера $2k$ не отделяются короткими монотонными схемами от $k$-раскрашиваемых графов. Кроме того, по опровержению в резолюциях формулы вида $A(x, y) \wedge B(x, z)$ можно построить монотонную схему, которая по данному $x$ говорит, что невыполнимо - $A(x, y)$ или $B(x, z)$. Теперь мы от противного строим схему для отделения графов с кликами от $k$-раскрашиваемых графов, подставив в Reflection Principle формулу $COL_k(G, q)$, которая проверяет, является ли $q$ правильной раскраской $G$ в $k$ цветов.