bramcohen (bramcohen) wrote,
@ 2006-03-19 09:22:00

**Improving Walksat**

I was thinking about Walksat recently and came up with an idea.

Let us consider 3sat only and start with the question: why does walksat work so well? Consider the model where we have only a single satisfying assignment, and some number of variables are right. With walksat, no matter what properties the problem has, the chances of walksat making a mistake if it picks a variable at random to flip (as opposed to trying to be clever and pick the heuristically guessed 'optimal' one) is at most 2/3. If that value were 1/2 or greater, as is the case in 2sat, then it would almost always find a solution quickly. In practice, being off by a mere 1/6 like that is pretty good. It's surprisingly difficult to come up with a technique which manages a hard cap like this - just about any heuristics you add can lead you in the exact wrong direction if the problem is appropriately structured.

Here's the breakdown of possibilities. If the selected false clause has one variable wrong, then the expected change in number of correct values is -1/3. If it has two variables wrong, the expected change is +1/3, and if three +1.

This expected change in number of correct variables approach leads to a few ideas. For example: instead of flipping just one variable, flip two. Then if there is one variable wrong the expected change is -2/3, if two the expected change is +2/3, and if three +2. These values are exactly double the values of only flipping one variable, so they have similar behavior but greater variance, which should, if we pretend this is a random walk, result in finding a solution faster. This technique also has the odd property that it doesn't change whether the number of variable set to true is even or odd, so it has to be run for either case. This is actually a big win - randomly searching two spaces of half size with a random walk requires on average a lot less steps than random walking a single space of double size, and it parallelizes perfectly.

Here's another idea: We have two cases, either (a) all variables in the selected clause are wrong, or (b) at least one of the variables in the selected clause is right. We'll have some tunable parameter which is the probability of dealing with the selected clause based on either assumption. If we guess (a), then we simply flip all three variables. If we guess (b), then we pick one variable which we think to be correct, and take all unsatisfied clauses which that variable appears in and flip one of the other two variables, picked at random. It's hard to fully analyze this heuristic, but it has a number of nice
properties - if you pick the everything is wrong case the probability distribution is similar to that in other heuristics, and if you pick the guess one is right case then if you pick a variable which you guess is right correctly then the expected change in correct assignments is guaranteed to be nonnegative.

All of these variants, unfortunately, suffer from the same basic weakness: if all unsatisfied clauses have two variables set correctly, you're on average going to take a step backwards. This especially becomes a problem as you get close to a solution.

Oddly, the wikipedia page on walksat doesn't contain either a link to the paper on it which I coauthored or a mention of me, even though I came up with the idea (of walksat, not gsat, which walksat is a slight variant of).

(Post a new comment)

leo1d
2006-03-20 05:47 am UTC (link)

no love for you with comments on this post. oh well, but you should just ask wikipedia to edit the entry for walksat. "where's my link darn it!" lol. but thank you for making bittorrent *bows down to you

(Reply to this)

ciphergoth
2006-03-23 01:08 pm UTC (link)

If it wasn't for that slight problem, it would be a solution to all problems in NP, so it's not that surprising really.

I wonder if there are situations where you could apply something like WalkSat to cryptanalysis?

(Reply to this) (Thread)

bramcohen
2006-03-23 07:01 pm UTC (link)

I wonder if there are situations where you could apply something like WalkSat to cryptanalysis?

Nothing which has happened since enigma - stuff which came before that, yeah, that stuff was very weak.

(Reply to this) (Parent) (Thread)

ciphergoth
2006-03-24 08:43 am UTC (link)
I'm currently trying to work out if there's a successive approximation strategy that will break Trivium - WalkSat alone is unlikely to do it, of course, but in combination with other techniques it might tip the balance. Just about everyone I spoke to at FSE 2006 is trying to break Trivium, of course :-)

(Reply to this) (Parent)