Social*Networks
QUIZ #4
B. Mishra

04 March 2014

Q1. [10] Three Wall-street Quants meet at a Bar in Manhattan. They want to figure out the average of their salaries; however, their contracts forbid them from disclosing their own salaries to each other. How can they do it?

SOLN.1 *Let us assume that the three co-workers are A, B, and C and their individual salaries are S_a, S_b, and S_c, respectively. They proceed along the following steps:*

- *A adds a random amount, say R_a to his own salary and gives that to B (B cannot know A's salary as the random amount, added is only known to A). In this case, B will receive the figure ($S_a + R_a$) from A.*
- *B does the same and gives the final amount to C (without showing that to A). Now C receives the figure ($S_a + R_a + S_b + R_b$).*
- *C does the same and gives the final figure to A (without showing it to B). Now, A receives the figure ($S_a + R_a + S_b + R_b + S_c + R_c$).*
- *Next A subtracts his random amount and gives the final figure to B (without showing that to C). B will now receive the figure ($S_a + S_b + R_b + S_c + R_c$).*
- *Next, B subtracts his random amount and gives the final figure to C (without showing it to A). C will receive the figure ($S_a + S_b + S_c + R_c$).*
- *Finally, C subtracts his random amount and then the figure becomes ($S_a + S_b + S_c$). It is shown to everyone so that any one of them can compute the average simply by dividing this figure by 3.*

It is important to note here that at every stage (except the very last where C subtracts his random amount), only two co-Quants communicating each other should know the fugures and not the third one.

Q2. [5] Will it work for any n number of quants?

SOLN.2 *Yes, except when $n \leq 2$, which are the trivial cases. For $n = 0$ and $= 1$, there is nothing to show. For $n = 2$, if A can find the average $Av = (S_a + S_b)/2$, then he can figure out B's salary as $S_b = 2Av - S_a$.*

Q3. [5] Can n Quants also figure out the probability distribution function (PDF) of their salaries without revealing their individual salaries?

SOLN.3 *Yes. Since they can use this trick to compute the moments:* $M_1 = \sum S_i$, $M_2 = \sum S_i^2$, $M_3 = \sum S_i^3$, *etc. One could argue that from the moments, one can solve for the individual salaries* S_i*; however, one still does not know which salary belongs to which Quant, as there is an ambiguity up to a permutation.*

The last point is interesting, and can be solved using Viete's formula and Newton's identity (and a bit of Galois Theory). Let

$$
\begin{aligned}
e_0(S_a, S_b, S_c) &= 1 \\
e_1(S_a, S_b, S_c) &= S_a + S_b + S_c \\
e_2(S_a, S_b, S_c) &= S_a S_b + S_b S_c + S_c S_a \\
e_3(S_a, S_b, S_c) &= S_a S_b S_c
\end{aligned}
$$

$$
\begin{aligned}
p_1(S_a, S_b, S_c) &= S_a + S_b + S_c \\
p_2(S_a, S_b, S_c) &= S_a^2 + S_b^2 + S_c^2 \\
p_3(S_a, S_b, S_c) &= S_a^3 + S_b^3 + S_c^3
\end{aligned}
$$

$$
\begin{aligned}
e_1(S_a, S_b, S_c) &= p_1(S_a, S_b, S_c) \\
2e_2(S_a, S_b, S_c) &= e_1(S_a, S_b, S_c) p_1(S_a, S_b, S_c) \\
&\quad - p_2(S_a, S_b, S_c) \\
3e_3(S_a, S_b, S_c) &= e_2(S_a, S_b, S_c) p_1(S_a, S_b, S_c) \\
&\quad - e_1(S_a, S_b, S_c) p_2(S_a, S_b, S_c) \\
&\quad p_3(S_a, S_b, S_c)
\end{aligned}
$$

The rest follows from the fact that we can now compute the salaries as roots of the following univariate polynomial:

$$
\begin{aligned}
&(t - S_a)(t - S_b)(t - S_c) \\
&\quad = \quad t^3 - e_1(S_a, S_b, S_c) t^2 + e_2(S_a, S_b, S_c) t - e_3(S_a, S_b, S_c).
\end{aligned}
$$

These arguments generalize to any n*.*