Conjecture C. What we have shown in Theorem A is that the improved lower bound has the order of magnitude $O(\ell^2)$.

Theorem A gives a sufficient condition for the truth of Conjecture C (and so are Conjecture A and B) in the case where $q = p$ a prime number and $\ell = \ell_0$. Thus, under the given sufficient condition an optimal CAC of length p with $4 \nmid o_p(2)$ and weight 3 has the desired size.

Corollary B. *Let p be an odd prime such that $4 \nmid o_p(2)$, let $\ell_0 = [\mathbb{F}_p^\times : H]$ and let $\omega(\ell_0), \delta$ be as in* Theorem A *with respect to ℓ_0. If $p \geq (2^{\omega(\ell_0)}(\ell_0 - 3 - \delta) + 2)^2 - 2$, then an optimal conflict-avoiding code of length p and weight* 3 *has the size*

$$\frac{p-1-2\ell_0}{4} + \left\lfloor \frac{\ell_0}{3} \right\rfloor.$$

Applying Corollary B, we can establish the truth of Conjecture C unconditionally for primes with small values of ℓ_0. For instance, if $1 \leq \ell_0 \leq 6$ then Conjecture C is true (see, Corollary 2.3, 4.4 and 4.5). Combining the results computed in [MZS14], Theorem A confirms the validity of Conjecture C for a large range of ℓ_0. For instance, if ℓ_0 is prime power satisfying $\ell_0 < 16411$ or if it has two distinct prime divisors such that $\ell_0 < 8197$ then Conjecture C is true for prime numbers p with ℓ_0 satisfying properties just stated (see Theorem 5.1 and Theorem 5.2 for more cases).

The organization of this note is as follows. In Section 2 we fix some notations and discuss some well-known facts related to Equation (3). In particular, by applying Hasse-Weil bound, we give a proof of the facts that Equation (3) is solvable over $\mathbb{F}_q$ in the case where $1 \leq \ell \leq 4$ (Corollary 2.3). Then, we collect and prove necessary results that are needed in the proof of the main result in Section 3. One of the key ingredients is *Ramanujan's sum* which we recall in Lemma 3.2. Section 4 is devoted to the proof of Theorem A. By appropriately organizing the character sum in the expression for the number of solutions to Equation (3), we are able to obtain the desired bound given in Theorem A for the number of solutions. In the final section, we apply our main result to the problem of the size of optimal CAC and deduce a large range of ℓ_0 such that Conjecture C (as well as Conjecture B and A) hold.

2. PRELIMINARIES

In this section, we fix notations and present some facts that are related to the question of solvability of Equation (3). Let $\mathbb{F}_q$ be a finite field of q elements where q is a power of the prime p. Fix a generator g of $\mathbb{F}_q^\times$ and a proper divisor ℓ of $q-1$. Let L be the subgroup of all ℓ-th power of elements of $\mathbb{F}_q^\times$. We have that $\mathbb{F}_q^\times/L$ is generated by the coset gL and ℓ is the order of the cyclic group $\mathbb{F}_q^\times/L$.

Recall that we're concerned with the solvability of Equation (3)

$$g^2X^\ell + gY^\ell + 1 = 0$$